Exhibits to iKeepSafe Comments

MB Docket No: 09-194

EXHIBIT A

Report of the Rochester Institute of Technology

Survey of Internet and At-risk Behaviors

Undertaken by School Districts of Monroe County New York

May 2007 to June 2008
October 2007 to January 2008

By Samuel C. McQuade III, Ph.D.
Graduate Program Coordinator

And

Neel Sampat, Graduate Research Assistant

RIT Center for Multidisciplinary Studies

June 18, 2008

Acknowledgments

The authors of this report wish to acknowledge and thank several individuals and organizations that made possible the *RIT Survey of Internet and At-Risk Behaviors*. Members of the Rochester Regional Cyber Safety and Ethics Initiative (RRCSEI) Executive Board who donated countless hours to help plan Initiative activities and procedures for surveying thousands of students along with hundreds of parents and teachers throughout Monroe County school districts. They are among a small group of educators, government officials and business people who understand the ways in which youth are now threatened and threatening each other online and the implications of this for social and educational reforms needed in society.

For their key leadership roles on the Executive Board and organizational support for the RRCSEI and RIT survey, the following individuals are recognized and thanked: Dr. Chris Manaseri, Superintendent of the Brighton Central School District; Jo Anne Antonacci, Deputy Superintendent Monroe-Orleans BOCES 2; Ed Suk, Executive Director of the New York Branch of the National Center for Missing and Exploited Children; Michael Miller, President of the Rochester InfraGard Member Alliance; and Allen Scalise, President of the Rochester Chapter of the Information Systems Security Association.

We also acknowledge and thank numerous individuals who represented and facilitated their districts' participation in the survey. These people included dozens of other school district superintendents, assistant and deputy superintendents, building principals and other district management team members, information technology service personnel, media enrichment staff, school counselors and teachers. Their combined efforts, and those of all members of the RRCSEI who participated in making this survey possible, have established a basis for Monroe County school districts to consider what can be done to prevent risky online behaviors by area students, and to do so in thoughtful dialog with parents and other members of the community.

Thanks are also extended to the 40,079 students and hundreds of parents and school district staff members who actually took the survey. They are thanked for taking the time and trouble to answer many questions, and for trusting RIT to respect their privacy and protect confidential responses to questions often of a very sensitive nature.

Organizations represented in the RRCSEI that also helped make this survey possible include the National Center for Missing and Exploited Children, the Information Systems Security Association, and the Rochester InfraGard Member Alliance. Special thanks are extended to Arbor Networks, Global Crossing, Great Lakes Networks, Symantec Corporation and Monroe-Orleans BOCES 2 all of which provided financial and/or in-kind support for the project. Chief among financial donors was Time Warner, Inc., which makes possible ongoing efforts of

the RRCSEI to promote cyber safety throughout upstate New York and beyond. Several organizational components of RIT also greatly assisted in and supported the study, namely the Center for Multidisciplinary Studies, the College of Applied Science and Technology, the Offices of Sponsored Research and Development, Community and Government Affairs, the Information Technology Services (ITS) Division, University News Services and the Office of the President. Members of RIT's Institutional Review and Office of Legal Affairs are also acknowledged and thanked for their careful review and approval of the survey. Without the involvement, assistance, guidance and support of all these units the survey would not have been possible.

Members of the research team included Dr. Samuel C. McQuade, principle investigator. Graduate Research Assistants were Nathan Fisk and Neel Sampat. Elizabeth Fisk served as an independent consultant, and Dr. Howard Shaffer and Dr. Richard Labrie, both of Cambria Health Alliance Division on Addictions (a Harvard Medical School teaching affiliate), provided technical assistance.

The full list of RRCSEI Advisory Board members include:

- Dr. Chris Manaseri, Superintendent, Brighton Central School District
- Jo Anne Antonacci, Deputy Superintendent, Monroe-Orleans BOCES 2
- Jim Colt, Director of Security, Monroe BOCES 1
- Mary Connery, Director, Fairport Central School District
- Tom Gallagher, Superintendent, Wheatland-Chili Central School District
- Susan Gray, Superintendent, Penfield Central School District
- Mark Laubacher, Director Communications and Technology, BOCES 2
- Dr. Sam McQuade, RIT/CAST/CMS Graduate Program Coordinator
- Michael J. Miller, Vice President, Security, Global Crossing; and President, Rochester InfraGard Member Alliance
- Amy S. Perry-DelCorvo, Assistant Superintendent for Technology and Information Services, Monroe BOCES 1
- Sister Elaine Poitras, Diocese of Rochester Department of Catholic Schools
- Allen Scalise, President, Great Lakes Networks LLC and President RochesterChapter Information Systems Security Association
- Dave Pecora, Associate Director RIT, Information Technology Services Division
- Fred Rion, Emergency Management Specialist, Monroe County
- Ed Suk, Executive Director New York Branch, National Center for Missing and Exploited Children

Together we are learning how to make cyberspace safer for children, youth, parents, school staff members and other people throughout our community.

Samuel C. McQuade III, Ph.D.
Principle Investigator

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In May 2007 through January 2008 fourteen Monroe County school districts in New York State participated in a major research study undertaken by the Rochester Institute of Technology (RIT). A major portion of the study was an online survey. It was designed to:

> Measure the nature and extent of online victimization and offending experiences of K-12th grade students;
>
> Determine types and levels of supervision and role modeling employed by parents pertaining to the use of computers and portable electronic devices by their children; and
>
> Obtain information from teachers about their perceptions of school-related cyber abuse and crime, along with the potential need and challenges associated with implementing cyber safety and ethics instruction.

The survey project was the initial basis for establishing a partnership among RIT and approximately thirty school districts from throughout the Greater Rochester New York area, along with three prominent national organizations, including: (1) the National Center for Missing and Exploited Children (NCMEC), (2) the Information Systems Security Association (ISSA), and (3) Rochester InfraGard Member Alliance. InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members.

These organizations initially joined forces in August of 2006 and eventually formed the Rochester Regional Cyber Safety and Ethics Initiative (RRCSEI). Monroe County school districts was actively involved in helping to create the RRCSEI, and shaping its mission of "advancing K-12 cyber safety and ethics education along with parent and workforce training in these topics through research, instructional programming, professional development, evaluation and public awareness." Thereafter, Monroe County districts and numerous other area school districts agreed during the fall months of 2006 to participate in what became the *RIT Survey of Internet and At-risk Behaviors.*

This report explains how the survey project was designed and administered. It summarizes the results of Monroe County districts' student, parent and teacher versions of the survey and makes recommendations for staff development, instructional intervention and outreach to parents. This report is one of three being provided by RIT to Monroe County districts as part the RRCSEI study. Other reports to be provided to districts are (1) a district level analysis of survey findings report and (2) a *Content Analysis Report* of available online instructional resources that school districts may wish to consider using as a basis for providing Internet safety, information security and cyber ethics education.

SUMMARY OF KEY FINDINGS

Most children now begin using the Internet while they are at Kindergarten age or even younger. As they age they use more information technology (IT) devices such as laptop computers and cell phones to go onto the Internet and for more purposes such as electronic gaming, to chat with friends, to complete school work, and conduct research or shop online.

Online activities of students in K-12th grades involve appropriate and inappropriate behaviors and Internet content.

Data reveal that the more time youth spend online the more likely they are to engage in or experience various types of cyber abuse and offending.

Data also reveal that unlike traditional stereotypes, the majority of cyber offenses involving children, adolescents and young adults are perpetrated by peers of approximately the same age or grade level.

Young students remain vulnerable to being abused online by strangers as well as by people they actually know including their own friends. The old paradigm of adults preying on children has been replaced with the new reality that kids now regularly prey on each other online.

Cyber abuse and offending by and among youth includes:

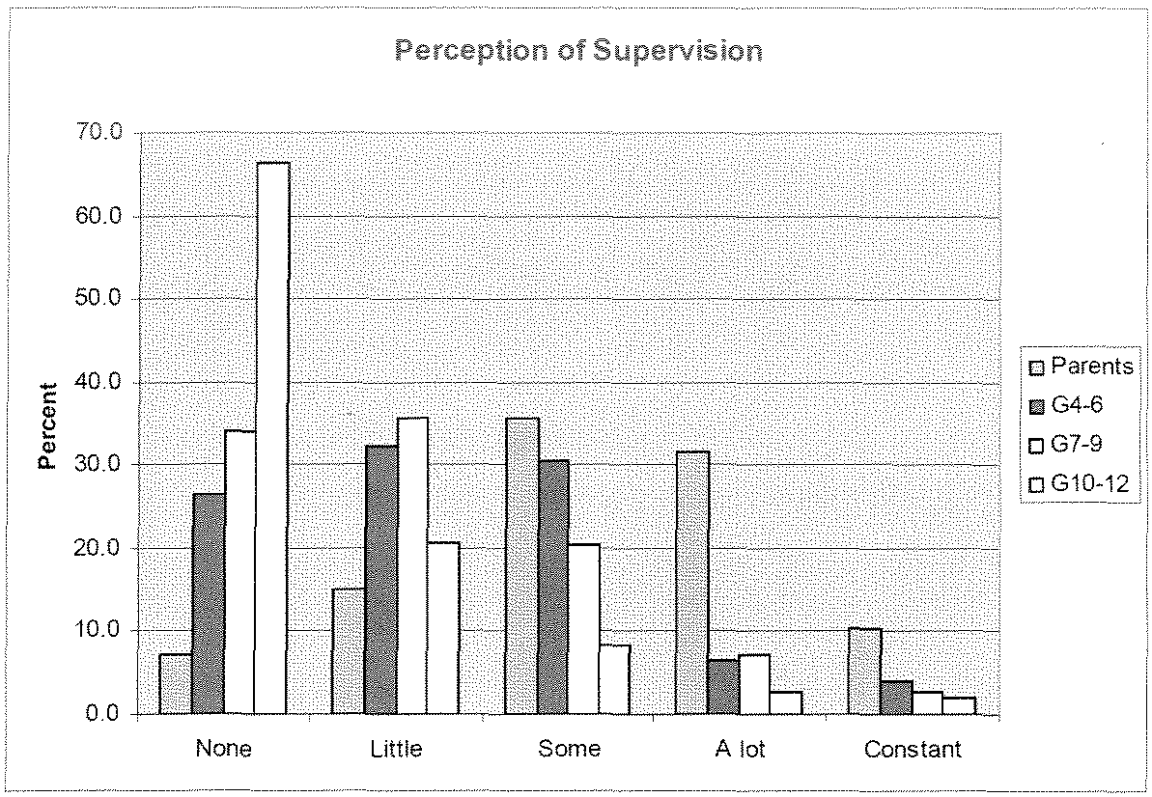
- Academic dishonesty such as cheating on assignments, and tests and plagiarism
- Cyber Bullying consisting of online embarrassment, harassment or threats
- Acquiring passwords and using computer systems without authorization
- Pirating of music, movies or software
- Lying about their age, appearance or identity often for social networking access
- Using credit card account information to commit fraud or access social networks
- Posting or sending indiscrete or nude photos and other personal data about themselves or other people online
- Sending sexual messages or solicitations for sex that are unwanted by recipients

Cyber bullying and victimization begins as early as the 2nd grade for some children. Illegal pirating of music, movie and/or software begins for many students in the 4th grade. By middle school students as a group experience and/or engage in all known forms of cyber abuse and offending.

Cyber bullying is prominent and also peaks in middle school, which is when online exchange of sex-related content begins. Cyber victimization, abuse and

crime generally continues and increases into high school years, which is when young adults begin to specialize in the forms of cyber offending (e.g., piracy, bullying and data snooping that involves activities like accessing computer systems without permission).

Survey findings reveal that students consistently believe they are less supervised than parents think they are. For example, while 66% of high school students reported that parents provide no supervision of their Internet activities, only 7% of parents surveyed reported that they provide no supervision.



Summary of Key Kindergarten-1st Grade Survey Findings:

- K-1st grade students access the Internet using various devices for a variety of purposes, including playing online games and communicating with other people. Online gaming is increasingly popular particularly among younger students.

- 48% of students at this grade level interact with people on Web sites, while only 50% indicate that their parents watch them when they use a computer, leaving the possibility of their being exposed to predation behaviors or other threats posed by online strangers or even persons they know or regard as friends.

- 48% reported viewing online content that made them feel uncomfortable, yet only 72% reported the experience to a grownup, meaning that one in four children did not.

Summary of Key 2nd – 3rd Grade Survey Findings:

- 2nd – 3rd grade students also access the Internet using various devices for a variety of purposes, including playing online games and communicating with other people. Online gaming is increasingly popular particularly among younger students.

- Only 32% of students surveyed report being watched by their parents when they go online.

- 9% report having been "mean to someone online" (cyber bullying) and 18% report that someone online has been mean to them, within the last school year.

- 38% report having been exposed online to something that made them feel uncomfortable, and only 70% indicated that they reported that incident to a grown up, meaning about three in 10 children did not.

- 13% of students report that they used the Internet to talk to people they do not know, 11% report having been asked to describe private things about their body and 10% have been exposed to private things about someone else's body.

Summary of Key 4th-6th Grade Survey Findings:

- 27% report that they are completely unsupervised when they go online, while 31% report they are watched by their parents "a little" or "sometimes."

- Frequently children in these grade levels engage in social networking activities. In the process, they post personal, potentially exploitable, information about themselves online. Specifically, and within the last school year: 16% posted personal interests online, 15% posted information about their physical activities and 20% gave out their real name. In addition, 5% posted information about their school, 6% posted their home address, 6% posted their phone number and 9% posted pictures of themselves.

- 5% of students reported they have been asked online to meet in-person, and 4% of students have asked to meet someone in-person on the basis of their online interactions.
- 12% reported someone pretended to be them online and 13% report someone having used their password or online account without their permission.

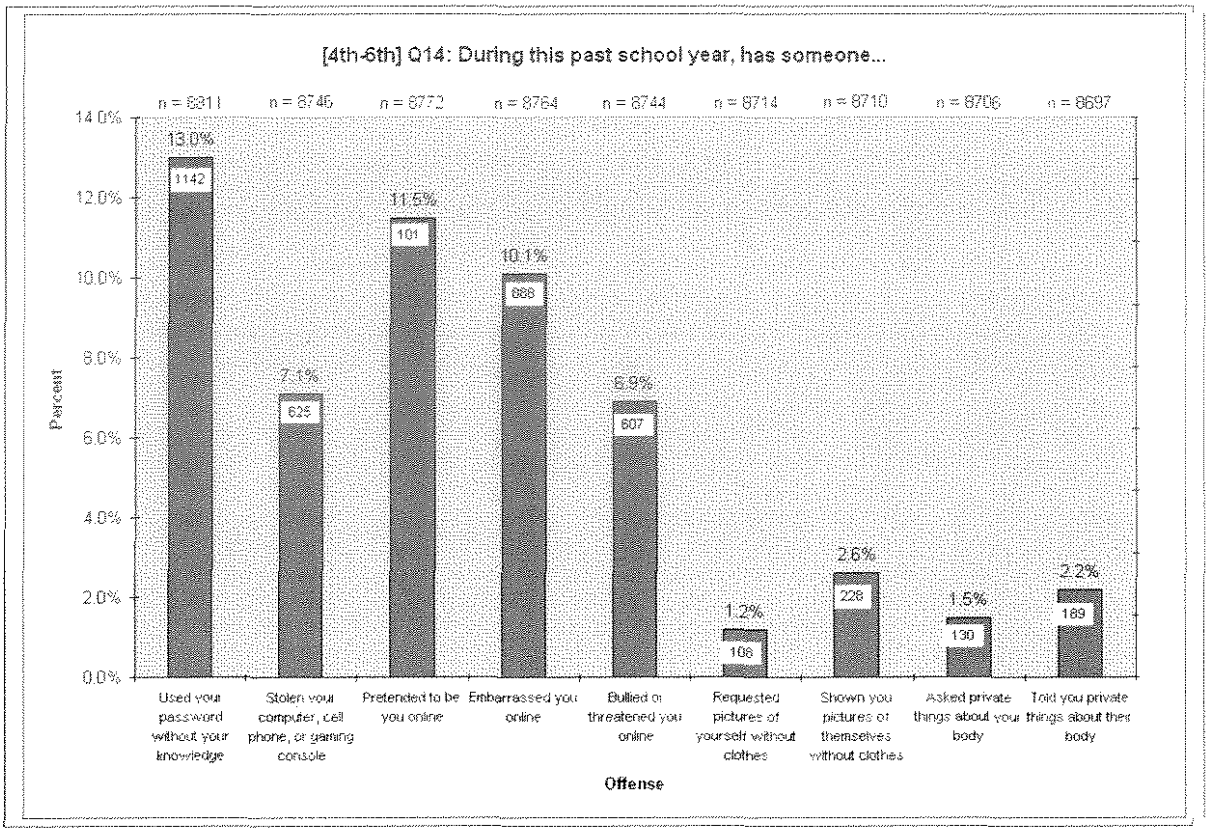
- 7% of students reported being the victim of cyber bullying/threats. However, 10% of students have been embarrassed online, which along with harassment is often an aspect of being bullied online.

- 2% report being exposed to nude photos of other people, 2% report being asked private things about their bodies and 1% were asked for nude pictures of themselves.

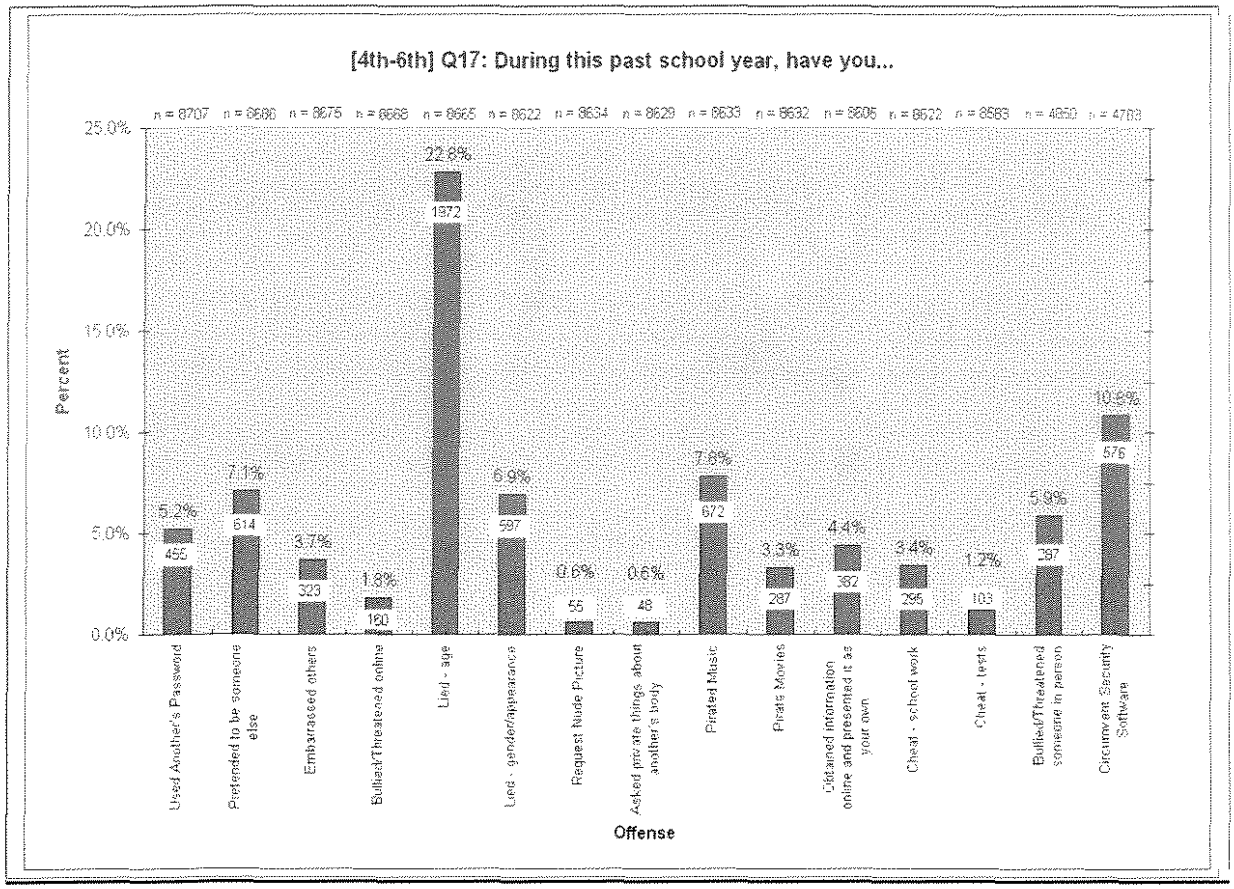
- Music, movie and software piracy often begins at this age. Within the last school year 8% of students reported they have downloaded music and 3% admitted to downloading movies without paying for these.

- Most victims report the perpetrator of their cyber abuse to be one of their peers, either a girl (in 27% of cases), a boy (in 25% of cases) or a friend they know in-person (36%). Only 16% did not know the person responsible for the cyber offense.

4th-6th Grade Victimization Chart



4th-6th Grade Offending Chart



Summary of Key 7th-9th Grade Survey Findings:

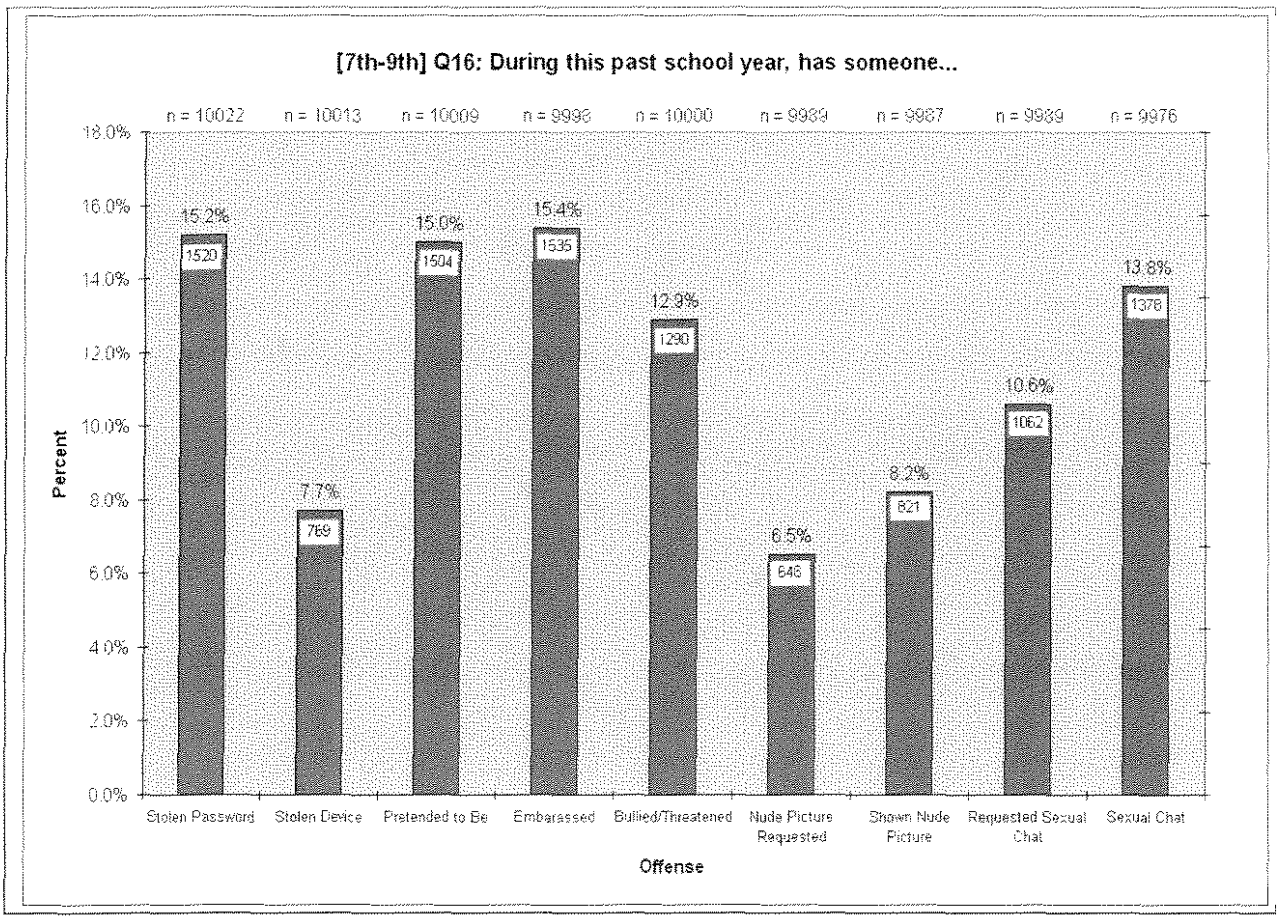
- As a group, 7th-12th grade students experience all known forms of cyber victimization and offending. Many individuals are victimized and/or commit various forms of online deceit, abuse or crime each year.
- 34% of middle school students report using the Internet with no supervision, another 36% report receiving only a little supervision.
- 42% report having spoken with at least one online stranger within the past year.
- 39% have posted photos of themselves, 36% have posted their real names, and 14% have posted their schedules and personal contact information.
- 9% have accepted an online invitation to meet someone in-person and 10% have asked someone online to meet them in-person.

- 15% have reported being embarrassed online and 13% indicate that they had been bullied or threatened online.

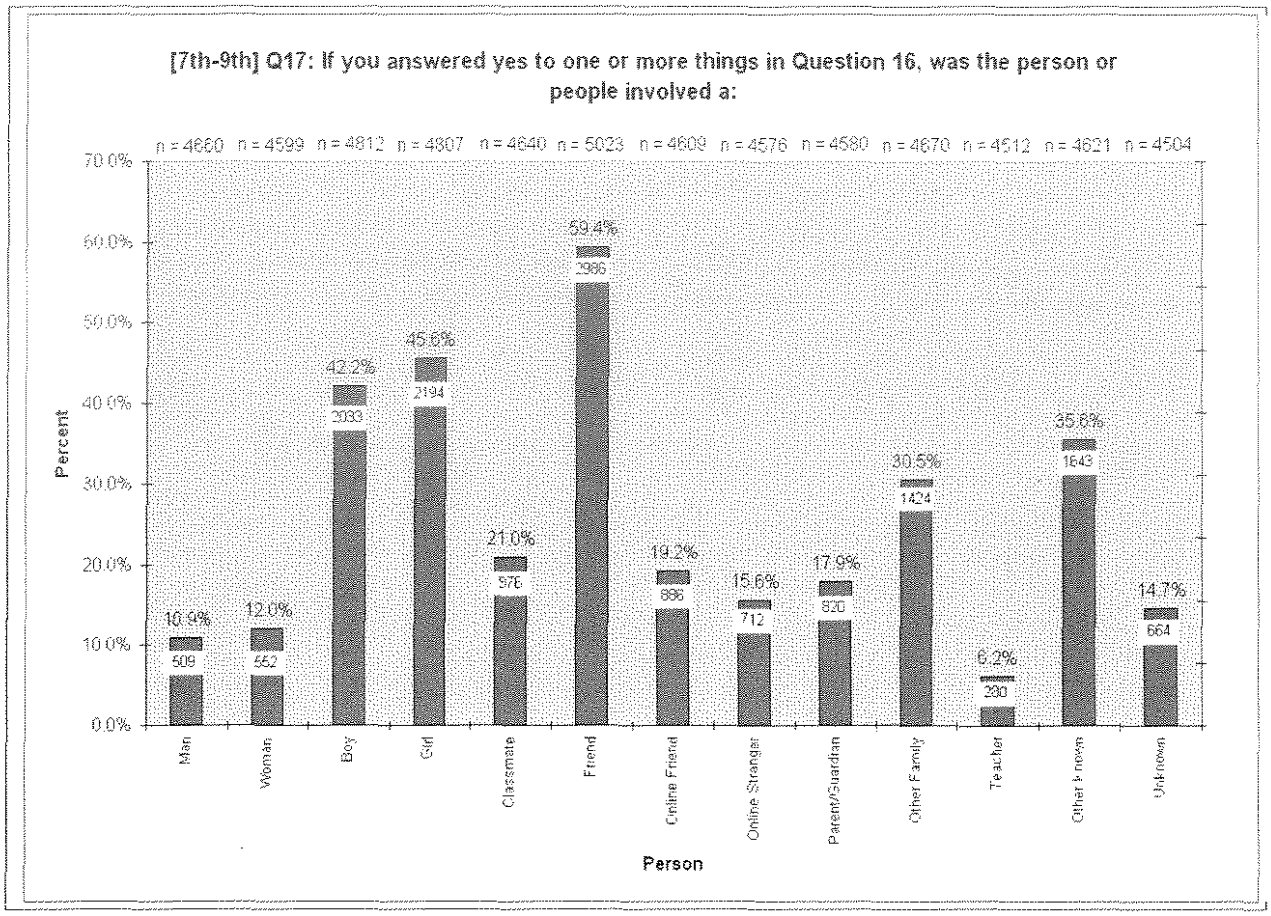
- 14% reported that they had communicated with someone online about sexual things; 11% of students reported that they had been asked to talk about sexual things online; 8% have been exposed to nude pictures; and 7% were also asked for nude pictures of themselves online.

- 59% of victims said their perpetrators were a friend they know in-person; 36% said it was someone else they know; 21% said the cyber offender was a classmate; 19% indicated the abuser was an online friend; and 16% said it was an online stranger.

7th – 9th Grade Victimization Chart



7TH – 9th Grade Known Perpetrator Chart



- Students are more likely to be victimized by other students rather than by adults. Further, when peers are identified as perpetrators of cyber offending, 46% of the time they are girls and 42% of the time they are boys. However, only about 12% of known cyber offenders were identified by students as being a man or a woman.

- 22% of middle school students downloaded music within the last school year that they did not pay for;

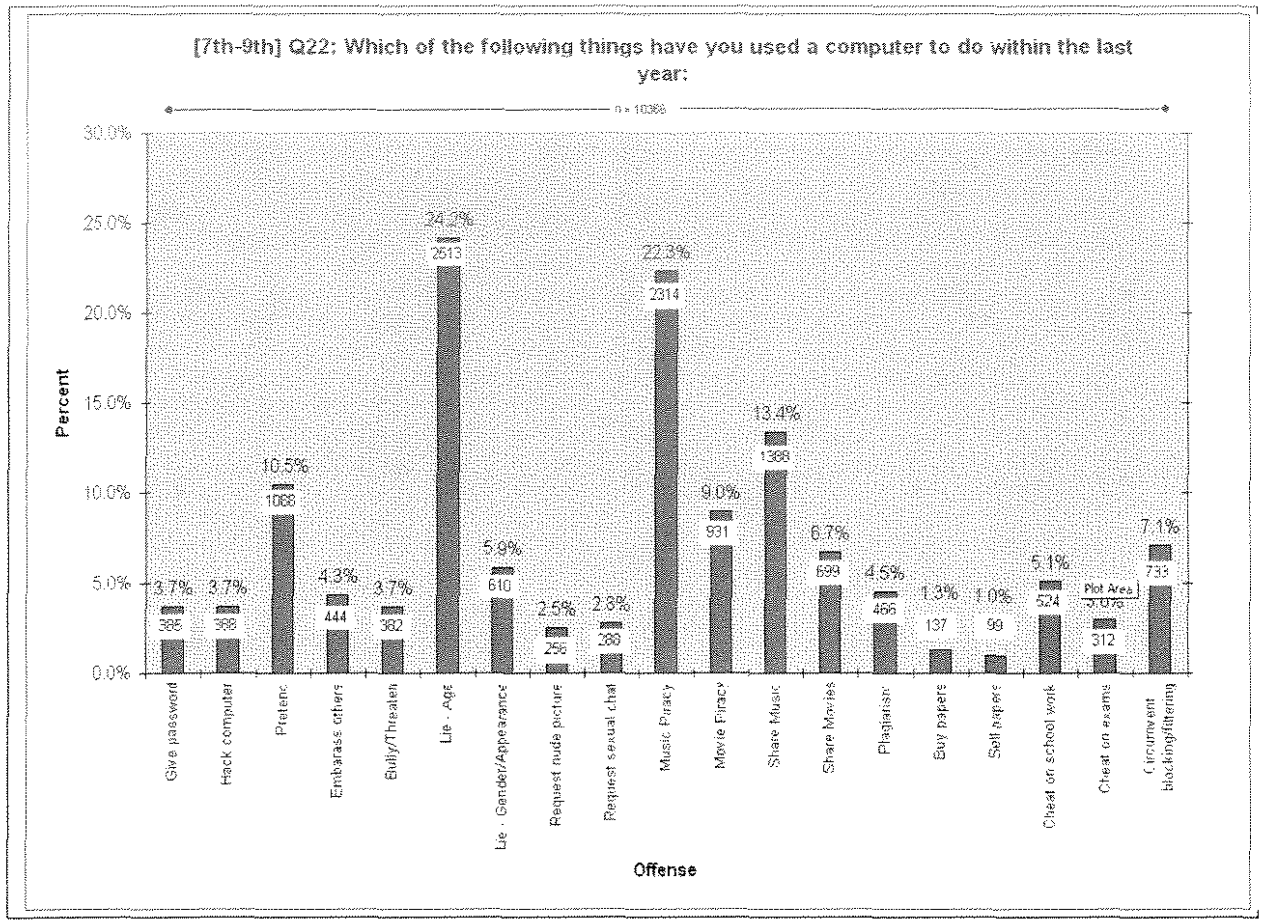
- 11% pretended to be someone else online, 4% admitted to intentionally embarrassing another person online and 4% admitted to harassing or threatening another person online.

- 3% admitted to asking for naked pictures from another Internet user and 3% also admitted to soliciting sexual chat online.

- 7% reported circumventing security measures designed to block or filter access to Internet web sites.

- Data also reveal various type of academic dishonesty. 5% admitted to online plagiarism; 5% admitted to cheating on school work; and 3% admitted to cheating on tests.

7th – 9th Grade Offending Chart



Summary of Key 10th-12th Grade Survey Findings

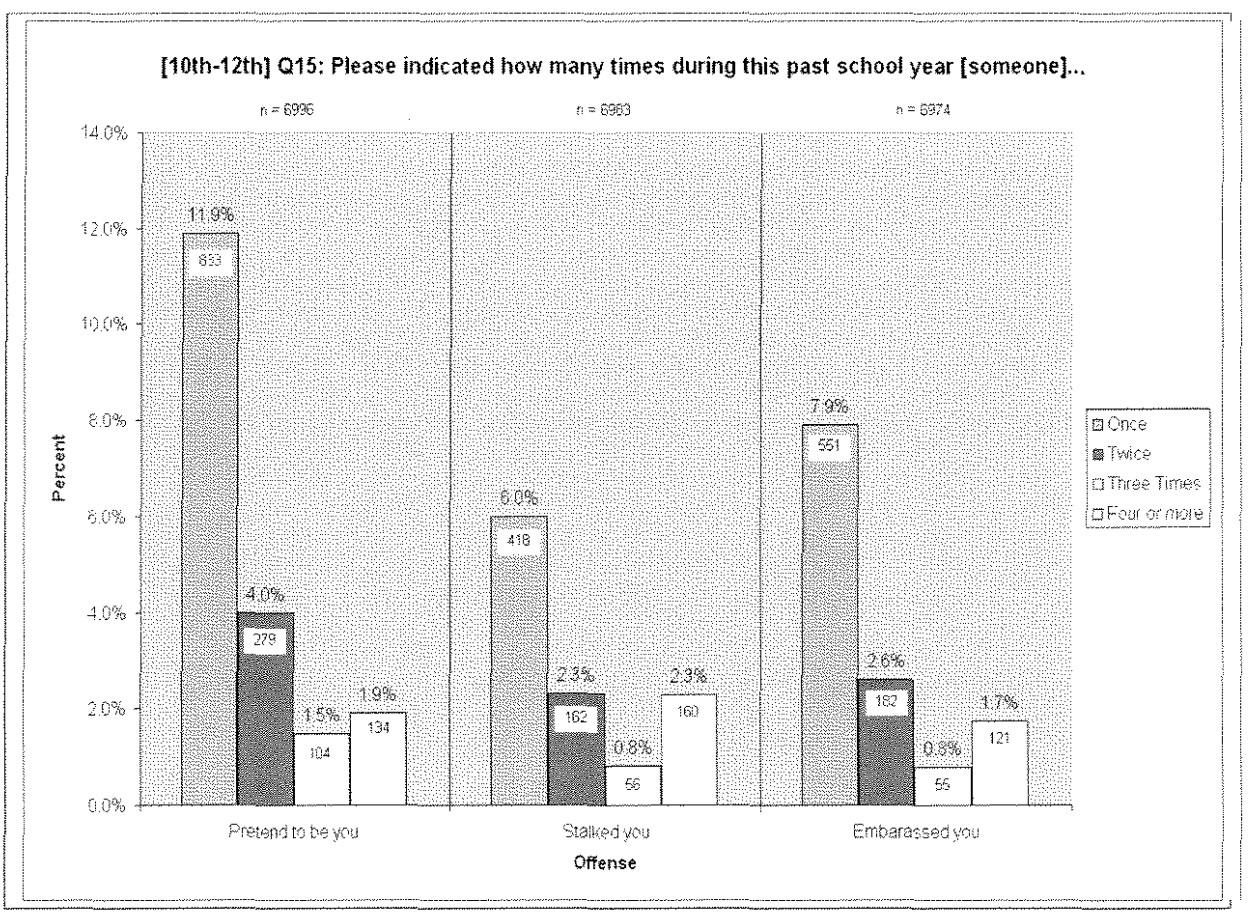
- Within the past year, many students indicated that they have used the Internet to interact with strangers in a variety of ways, including: chatting 48%; flirting 25%; providing personal information 22%; talking about private things 17%; and engaging in sexually oriented chat 15%.

- 14% have accepted an invitation to meet an online stranger in-person and 14% of students, who are usually the same individuals, have invited an online stranger to meet them in-person.

- 16% have experienced cyber bullying; 17% have been embarrassed online; and 15% have been harassed or stalked online.

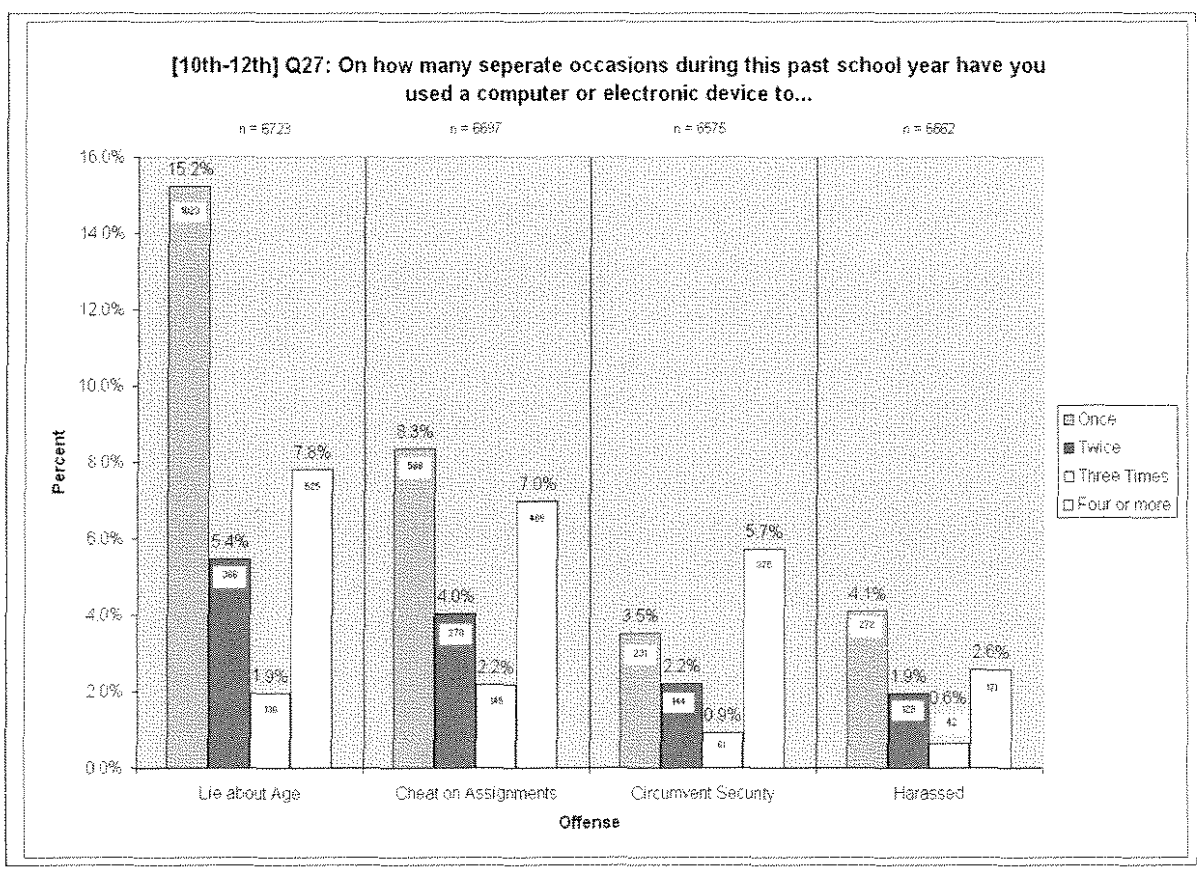
- 23% have been exposed to unwanted pornography and 23% have been asked about sexual things online.

10th-12th Grade Multiple Victimization within Preceding Year (Selected Types of Offenses)



- 21% admitted using a computer or electronic device to cheat on a school assignment within the last school year. 12% admitted plagiarism and 9% reported having used a device to cheat on an exam.
- 65% have illegally downloaded music in the past year; 34% have illegally downloaded movies and 30% have illegally downloaded software.
- 12% of students in high school reported they circumvented computer security systems designed to filter or block their access to Internet web sites.
- 9% have admitted to harassing someone online and 8% have admitted to threatening someone online within the past year.

10th-12th Grade Multiple Offending within Previous Year (Selected Types of Offenses)



Summary of Key Parent Survey Findings

- 47% (n=376) of parents surveyed report that they enjoy using computers "A lot".
- On average, parents report that there are three different kinds of computing devices owned by members of their household.
- 82% of parents report that their children routinely use desktop computers and 20% report that their children use laptop computers.
- 30% of parents surveyed indicated that their children routinely use a cell phone.
- 25% of parents feel that their child knows more about computer technology than they do, while 14% feel that they know the same about computers as their children do.
- 90% of parents surveyed indicated that there is an adult present to supervise home computing activities of their children.
- Parents generally are aware of flitering, blocking and information security software, but only 30% of parents surveyed reported they use these types of software.
- 61% of parents surveyed indicated their children access the Internet from a private place in the home.
- The most commonly observed computing activity by parents of their children was school research (reported by 76% of parents), playing video games (reported by 61% of parents) and watching movies or listening to music (reported by about 50% of parents).
- 14% of parents have caught their children doing something with a computer device that they should not have been doing.

Summary of Key Teacher Survey Findings

- A total of 889 teachers and other school district staff responded to their version of the survey.

- In general they feel that their school districts are well prepared to facilitate student learning through technology. Many faculty report using computer technology to facilitate learning in their classrooms.

- Faculty vary in the amount of professional training and education they have received about information security and technology.

- Relatively few teachers believe they are currently prepared to teach students in areas of Internet safety, information security or cyber ethics, though a majority believe these are important subjects for students to know. However, teachers of grades K-3 generally believe that these subjects are less important for younger students to know.

- School staff are divided in their perceptions about whether students know more about information technologies than they do, regarding whether student use of electronic devices in school are problematic, about their ability to supervise Internet activities of students on school property, and with regard to knowing what steps and capabilities their districts have to guard against inappropriate Internet activities of students.

SURVEY DESIGN AND ADMINISTRATION PROCEDURES

The *RIT Survey of Internet and At-risk Behaviors* was funded with single (onetime) contributions of $2,000 from each of approximately twenty school districts most, of which elected to participate in surveying. These funds were provided to RIT through Monroe-Orleans BOCES 2 which serves as the lead school district for providing administrative support to the RRCSEI. Funding support was also provided by corporate and individual donors (see Acknowledgments), and through in-kind services provided by several organizational components of RIT as well as Monroe-Orleans BOCES 2.

In August 2006 representatives from area school districts and the NCMEC, ISSA and InfraGard met for the first time to begin developing plans for the survey project. By December a total of seven online survey instruments had been developed. Five instruments consisted of questions designed for students in the following developmentally distinct age/grade levels: K-1st grade; 2nd-3rd grade; 4th -6th grade; 7th-9th grade; and 10th-12th grade. Two additional survey instruments were developed: one for school district teachers and other staff, and another for parents of school district students. All instruments were designed for online survey administration using WebSurveyor software that was procured by RIT specifically for this project.

Specific survey questions were developed by RIT researchers under the direction of Dr. Samuel C. McQuade, the project's Principal Investigator. He and his colleagues were assisted by a large RRCSEI advisory team collectively familiar with lay literature and scholarly research bearing on cybercrime, online child victimization and education administration issues. Subject matter experts and consultants retained for the study were also involved in survey instrument design, review and testing. These individuals were drawn from the Cambria Health Alliance Division on Addictions (a Harvard Medical School teaching affiliate) and local area organizations known for staff expertise in research methods, human and early childhood development and school psychology.

The combined expertise of approximately 35 professionals representing or drawn from school districts and other organizations spanned several academic fields. Fields of expertise included: human development and child psychology; primary and secondary education instruction; school psychology and education administration; criminology and criminal justice systems administration; sociology and online social networking, information technology systems security and network administration; public administration; and public policy among other fields of expertise. The eclectic expertise of the researchers and advisory team resulted in a very sophisticated and multidisciplinary study design consisting of the largest, most comprehensive and in-depth sets of questions ever developed to examine issues related to the prevention of online abuse, offending and victimization.

Following their initial development all seven survey instruments were distributed for review and comment to RRCSEI members including school district representatives (approximately fifty professionals in all), representing numerous school districts and organizations affiliated with the project. They subsequently recommended content, structure and wording changes. Survey instruments were then revised several times until the RRCSEI membership agreed on the design and wording of questions in all seven instruments. Following this review and approval all survey instruments were then time-tested in February 2007. This was accomplished using paper (hardcopy) versions with small focus groups of individuals purposively selected from within the Fairport Central School District (parents and teachers), the Rush Henrietta School District (10^{th}-12^{th} graders), and the Diocese of Rochester schools (K-9^{th} graders).

Time testing revealed that all surveys could be administered and completed within 30 minutes (the acceptable maximum as determined in advance by school district representatives to the RRCSEI). Field observations of time tests coupled with informal post-survey focus group interviewing by RRCSEI/research team members resulted in additional minor changes to the structure, content and wording of survey instruments. Field testing also enabled researchers to understand how best to administer surveys to K-3rd grade children who were necessarily scheduled to complete audible ("talking computer") survey questions using headphones.

Following time-testing in the field the entire research study, including all final survey instruments, was reviewed and approved by RIT's Institutional Review Board (IRB). (See surveys in Appendices A-G.) In its decision to approve the study the IRB carefully considered the importance of the research as balanced against potential risks to children and adult survey takers, along with matters pertaining to parental consent and child assent (i.e., voluntariness), privacy and data security among several other issues. As part of the overall IRB review the study was also determined by RIT's Office of General Counsel to comply with federal regulations governing research involving human subjects. The study was also reviewed by the law firm of Harris Beach representing Monroe-Orleans BOCES 2 (and certain other school districts) and determined to be in full compliance with New York State education and student privacy laws.

With IRB and legal approvals secured, researchers began in April 2007 to provide survey administration training to designated school district staff. This training consisted of approximately two-hours of on-site instruction and computer demonstrations that addressed key procedural issues likely to be encountered by school district personnel when administering surveys to students. The goal was to provide designated individuals and teams of district representatives with sufficient information to replicate the training for other district staff as needed to accomplish surveying within designated school buildings. (See training presentation outline in Appendix H.)

As training was being provided to school district personnel, districts also began notifying other staff and parents of the impending surveys. Parents were notified with standardized cover letters that were developed by RIT and sent by districts as U.S. Mail. Included with the letters was the *Parent Notice and Permission for Minor to Participate in Researc*h form that was also developed by RIT and reviewed by the RIT-IRB. The letter and parent notice included background information about the survey; referred parents to the RRCSEI website (www.rrcsei.org) for examples of complete survey instruments and questions to be asked of students, parents and school staff; and explained opt-out procedures parents needed to follow if they preferred their children not participate in the survey.

Brighton, Diocese of Rochester, East Irondequiot, Fairport and Newark school districts surveyed students, parents and teachers beginning in May 2007 . Students completed surveys under staff/adult supervision during normal school hours in computer-equipped classrooms, libraries or computer labs. Other school districts began surveying in September 2007 (BOCES 1, Canandaigua, Greece, Hilton, Penfield, Pittsford, Rush-Henrietta, Webster and Wheatland-Chili). Taken together these districts represented urban, urban-bordering, suburban and rural schools located in Greater Rochester and upstate New York. The combined number of pilot surveys (spring 2007) and fall/winter responses (September 2007 – January 2008) in fourteen districts was 40,079 students, 889 teachers and 365 parents.

DISCUSSION OF SURVEY RESULTS

Monroe County school districts that completed the *RIT Survey of Internet and At-risk Behaviors* had an overall large sample. Of the 40,369 who initially accessed the informed consent and assent information, 40,079 students actually completed their version of the survey. Thus, the overall County response rate was 57% of an estimated 70,314 students enrolled in Monroe County school districts surveyed from spring-fall of 2007 into January 2008.

Within every grade cohort level responses were split evenly across gender lines with approximately 50% female and 50% male students in all grade cohorts. Barring extreme outliers within the higher grade levels, the reported ages of students taking surveys fell within customary age ranges (e.g. K-1st students were 5, 6, or 7 years of age.)

By way of further introducing survey results specific to each set of grade levels surveyed, readers of this report should understand that the data presented here are summaries primary (i.e., descriptive level) findings. This includes information that generally corresponds to most but not all survey questions in the order they were asked in each survey instrument (see Appendices A-G). Since more and more in-depth questions were asked of older students, reported findings and discussion of these in the following sections generally becomes longer and more complex. In all instances however, data reveal online experiences, perceptions and/or threats as reported by students, teachers and parents. As such the following sections are intended to guide decision-making in cyber-related education matters. They do not, however, include discussion of secondary analysis pertaining to more academic issues like profiles of particular types of cyber offenders or victims, or how such profiles correlate with reported substance abuse, social computing or indicators of so-called "computer/Internet addiction," and so forth.

Lastly, when reading through the following data summaries, readers should keep in mind that the number of students of an age/grade cohort who initially accessed the survey may not have assented to answer any questions or some of the questions asked. Students were also allowed to stop taking the survey at any time and in most instances allowed to skip particular questions if they chose to. Consequently, response rates varied from one question to another. These differences are reported within parentheses that indicate the percentage of students among the number who answered a question in the particular way indicated. For example, suppose 1,000 students within an age/grade cohort initially accessed the survey but only 950 assented to voluntarily answer questions (i.e., "take the survey"). If only 850 students answered a given question of which 750 answered "YES" in response to that particular question, then the report will say that 750 students or 88% of them (i.e., 88%, of n=850) answered the question affirmatively. All statistics are rounded down to the nearest whole number.

Kindergarten – 1st Grade

A majority of Monroe County school district students in K-1st grade reported they have access to and use a computer while at home (91% of n=4,747 students who answered this question). Of students who do, (63% of n=4,459) reported they use their home computer to access the Internet. By extrapolation (.91 x .63), approximately 57% of K-1st graders attending Monroe County districts connect to the Internet while using a computer in their home. When they do, these students access a variety of content in connection with several different types of online activities.

The most prominent Internet activity engaged in by children in this age/grade level cohort is online gaming with 92% (n=2,796) of children reporting they "play games on kids websites." Additionally, 66% (n=2,794) of Monroe County district K-1st graders "listen to music or watch videos" online, 48% (n=2,788) "read or write e-mail", 48% (n=2,792) "look on websites for schoolwork" and 41% (n=2,792) "talk with people on a website." These survey findings confirm that substantial proportions of very young children are immersing themselves in interactive media, and that their use of computers and the Internet is an integral aspect of their lives.

Fully 70% (n=2,784) of K-1st grade students surveyed reported that when they are connected to the Internet from home they "use the computer for a long time" rather than a "short time." Many students at this level also report that they go online unsupervised as revealed by only 50% (n=2,784) indicating that their "parents watch them when they use the computer." Note however, that the survey methodology cannot differentiate child perceptions of supervision with actual levels or means of supervision employed by parents (or other grownups in households). Still, the percentage of students who report their parents do not watch while they use their home computer (and presumably also when they use the Internet) is underscored by only 61% (n=2,785) of students reporting they are limited by their parents in the amount of time they are allowed to use computers at home. This is in contrast to 30% (n=2,785) of K-1st graders who reported they are watched by their parents when using their home computer and also limited in the amount of time they are allowed to use the computer.

As indicated above, some students use the Internet to communicate with other people. This reality reveals the possibility of their being exposed to predaory behaviors or other threats posed by online strangers or even persons they know or regard as online "friends." In addition, survey data cannot make clear whether students who report that they "talk with people on a website" are actually communicating with real people versus animated (virtual) characters, or whether these subjects are real people actually known in-person by the child. However, of the 48% (n=2,775) of K-1st graders who reported viewing online content that

made them feel uncomfortable, only 72% (n=1,307) reported the experience to a grownup.

The preceding findings reflect answers from all sixteen questions asked of Kindergarten and 1st grade students. Data clearly indicate that about half of Monroe County districts' students who are between four and seven years of age use a home computer to access the Internet, engage in various online activities, experience various types of content (some of which makes them feel uncomfortable), and quite probably in many instances do so without adequate levels and/or methods of parental supervision.

Charts and tables of these data are provided in Appendix J.

2nd–3rd Grade

Results of 2nd-3rd graders who participated in the survey resemble those of the younger age cohort described above. Sixty-Seven percent (67%, n=5,540) of students surveyed reported having Internet access from some location not limited to their home, and by using a variety of electronic devices, including: computers (96%, n=3,689); cell phones (14%, n=3,670); home video game consoles (21%, n=3,676); and/or portable video game consoles (23%, n=3,665).

As with their younger counterparts, a majority of 2nd-3rd graders engage in online gaming (94%, n=3,676) among other types of online activities. However, at these grade levels the same amount of students proportionately reported accessing online music and video content (60%, n=3,668) in comparison to the K-1st cohort, while the same percentage reported they access websites for schoolwork (36%, n=3,664) or to communicate with other people online (specifically with family or friends online at 37%, n=3,667).

These findings are consistent with the reality that many students within this grade cohort are only beginning to read/write and thus limited in their ability to understand text-based Internet content to establish communication channels. Within this age/grade cohort, the percentage of students who report being watched by their parents when they go online decreases to 32% (n=3,665). A little over half of 2-3rd grade children surveyed report their parents limit the amount of time they can spend online (50%, n=3,658)[1].

As students acquire skills necessary to communicate with each other online and begin to do so, the potential for cyber bullying increases. Survey data show that

---

1

[1] Specific reasons for the drop in parental supervision are unclear, although it is well understood that parents have more confidence in their children as they age. Thus, if the previous (K-1st) cohort data were applied retrospectively to this cohort, a majority of 2-3rd graders who took the survey in spring 2007 actually began using their home computers to access the Internet when they were younger and arguably are now in need of less supervision. This same principle holds for all students: as they age they need less supervision, and when older may require greater levels of privacy with regard to their use of computers and portable IT devices.

9% (n=3,676) of students at this age/grade level report having been "mean to someone online" with 18% (n=3,671) reporting that someone online has been mean to them.

Some students are experiencing both cyber bullying roles, with 2% (n=3,671) reporting that they have been mean and also have had someone been mean to them online within the last year. Thus, the age of onset for cyber bullying (that which may eventually escalate into some combination of online threats, harassment, intimidation or intentional embarrassment) appears to begin for some students in the 2nd grade. However, here again, readers should interpret these data cautiously, because the survey questions do allow for discernment of "how mean" or "in what ways" being mean online occurs at this age/grade level.

While online 38% (n=3,568) of Monroe County school district 2-3rd graders report having been exposed to something that made them feel uncomfortable. The exposure to online strangers is clear, with 13% (n=3,671) of students reporting that they used the Internet to "talk with people… [they] do not know."

Additionally, 11% (n=3,654) reported having been asked to describe "private things about [their] body" and 10% (n=3,656) have been exposed to "private things about [someone else's] body." Note that as previously indicated, such content may have been provided by someone the child actually knows and interacts with offline, or does not know either directly or incidentally (e.g., via a website), just depending on how the child interpreted the following specific survey questions:

> Q28. Has someone online on the Internet ever asked you private things about your body? (Answer choices: Yes or No.)
>
> Q29. Has someone online on the Internet ever told or shown you private things about their body? (Answer choices: Yes or No.)

Given this context and from data analyzed for older age/grade level cohorts (see below), it appears likely that many Monroe County school district students are being exposed to Internet communications of a sexual nature by the 2nd grade if not earlier in life. Most students in the 2-3rd grade who reported having experienced Internet content that made them feel uncomfortable (70%, n=3,646) also indicated they reported the incident to a grownup. However, about three in ten children do not for reasons that are unclear.

Charts and tables of 2-3rd grade data are provided in Appendix K.

4th–6th Grade

Students within this grade cohort also began using computers and the Internet at an early age, and data analyzed across the grade cohorts (and from other

studies) indicate that every year larger proportions of students are introduced to computers and the Internet at younger ages. Indeed, 4th-6th graders who participated in this survey reported that they started using computers at an average age of five, with 30% (n=8,736) indicating their computer use began at age four or even earlier. Most students reported they learned to use computers from parents (44%, n=9,351) or were self-taught (16%, n=9,351), although 16% indicated they were taught by teachers (n=9,351). Lesser proportions of students surveyed reported learning how to use computers from friends, siblings or other people.

Students at this age/grade level also use various devices to access the Internet and thereby reveal a range of technical computing abilities. On average, 4th-6th graders use more than two different types of devices to access the Internet. Desktop (91%, n=8861) and laptop (49%, n=8,244) computers are the devices most commonly used. However, two in five students (n=8,056) use video game consoles for Internet access, and 12%, n=7,905) use cell phones to access the Internet.

Kids' websites, music, videos and games remain the biggest attractions for students at this age/grade level. About 92% (n=8,744) of 4-6th graders reported that they engage in some form of online gaming, while 87% (n=8,643) are visiting kids' websites. Approximately 38% of 4th-6th graders instant message (n=8,417) and 54% e-mail (n=8,463) other people. 26% of students use chat rooms (n=8,330) and 24% text message (n=8,293).

As these students venture online to communicate with peers, family and either intentionally or unintentionally with strangers, parental supervision is critical. The majority of 4th-6th grade respondents indicated that their parents do supervise them to some extent, with 27% (n=8,972) having reported that they are completely unsupervised online. 31% (n=8,972) reported they are watched by their parents "a little" or "sometimes."

Slightly less than half of 4th-6th grade students (n=8,905) report they are limited by their parents in the amount of time they spend online; Internet access appears to occur more frequently from public locations within residences that are more easily supervised such as a kitchen or living room rather than a bedroom. Nonetheless, 4th-6th graders believe they are not closely supervised online, and may not be with respect to actual monitoring by parents of online activities, time spent online and/or location from which the Internet is accessed. Conversely, many opportunities for supervised Internet access exist but appear to be underutilized by many parents. At an age when students are just beginning to solidify offline and online social networks and form concepts of appropriate and inappropriate online behavior, this is a major concern because children alone cannot be relied on to achieve ethical underpinnings for civil behaviors deemed appropriate in society.

Participation in online risky behaviors, such as posting sensitive information online and arranging while online to meet people in-person is relatively low among 4th-6th grade students. Some forms of personal information are more likely to be posted including personal interests (16%, n=8,757), physical activities (15%, n=8,743) and real name (20%, n=8,742). Others forms of potentially exploitable information are also posted by students including information about their school (5%, n=8,724), real home address (6%, n=8,708), phone number (6%, n=8,696) and pictures of themselves (9%, n=8,707). Only a very small percentage of students report they have been asked by people online (not necessarily by strangers) to meet with them in-person (5%, n=8,676), or have asked people online to meet them in-person (4%, n=8,668). While participation in risky behavior online may be low, there are still a significant number of students who participate in each form of behavior measured, each of whom may face increased risk of victimization due to posting of personal information online.

The majority of students (84%, n=9,351) within this grade cohort have not experienced any form of online victimization measured by the survey within the past school year. However, 16% (n=8,743) indicated that they experienced one form of victimization, and 12% report they experienced two or more forms (see Appendix C, 4th-6th grade survey instrument, Question 14). Of the nine forms of victimization measured, the most prevalent were: "someone used their password without permission" (13%, n=8,811) and someone pretended to be them online (12%, n=8,772). Experiences with online embarrassment (10%, n=8,764) and online bullying/threats were experienced by 7% of students (n=8,744).

Online sex-related victimization experienced by 4th-6th grade students was also generally low: exposure to nude photos and being told private things about someone else's body was reported by 2% of students (n=8,706), being asked sensitive questions about their own body was reported by 2% (n=8,697) of students. 1% (n=8,714) of student respondents were asked to send pictures of themselves without any clothes and 3% (n=8,710) were shown pictures of other people online without their clothes on.

Contrary to the commonsense notion that online strangers are responsible for initiating inappropriate or unwanted sexual communications, among other types of online abuse or crime, many students who were victimized reported they actually know the perpetrator(s) as a real person they interact with offline as well as online. For example, when asked to characterize the person responsible for the type of incident they experienced, students most commonly reported a "boy" (25%, n=3,400), "girl" (27%, n=3,356) or "friend [they] know in person" (36%, n=3,420). In contrast, comparatively few students responded that the person responsible was an adult "man" (8%, n=3,347) or "woman" (7%, n=3,272), and only 16% (n=3,138) did not know the person responsible.

It follows that if students within this grade cohort are victimized by friends their own age, the same students may also engage in abusive behaviors using computers, other types of electronic devices and the Internet. Survey data indicate that this is indeed the case with substantial numbers of 4th-6th grade students having reported that within the preceding year they engaged in each of the 14 forms of deceptive, abusive or criminal behavior asked about (see Appendix C, 4th-6th grade survey instrument, Question 17).

The most common form of deceptive behavior indicated is lying about age online (23%, n=8,665). Other forms of online deceit are less common, e.g.: pretending to be someone else online (7%, n=8,686); lying about gender or appearance (7%, n=8,622); and online plagiarism (4%, n=8,605). Additionally, survey data reveal that for many students music and movie piracy may begin at this age/grade level, with 8% (n=8,633) admitting to having downloaded music and 3% (n=8,632) having downloaded movies without paying for these. Very few students admitted having bullied or threatened someone online (2%, n=8,668) and reported engaging in sex-related behaviors online such as requesting nude pictures (0.6%, n=8,634) and asking private things about another person's body (0.6%, n=8,629).

Charts and tables of 4th-6th grade data are provided in Appendix L.

7th-9th Grade

Within this grade cohort survey data reinforce the reality that students are being consistently introduced to computers at younger ages. On average students remember beginning to use computers at seven years of age (n=10,050) with 35% (n=10,366) indicating that their parents taught them the most about computers. Clearly parents continue to have a vital opportunity and role to positively influence responsible use of computers, other electronic devices and the Internet by students as they prepare for and enter school systems.

As with younger grade cohorts, 7-9th grade students use different types of devices to access the Internet, including: desktop computers (93%, n=10,365), laptop computers (57%, n=10,366) and more expansive use of cell phones (26%, n=10,366). Slightly greater numbers of students at this age/grade level use gaming consoles (24%, n=10,366). Devices used by students are for various purposes, but interactive communication with other people is more prevalent than with younger aged students.

72% (n=10,366) of 7-9th graders report using the Internet to instant message and 73% (n=10,366) e-mail, and many are also text messaging (48%, n=10,366) and using social networking sites (45%, n=10,366). Retrieving online videos and music (85%, n=10,366), school research (76%, n=10,366) and web browsing (71%, n=10,366) were also reported to be common activities, although online

gaming lessens to about 71% (n=10,366). Of the types of online activities measured, 7th-9th grade students were least likely to participate in chat rooms (25%, n=10,366) or create websites (18%, n=10,366).

Continuing the trend of less supervision at higher grade levels, 34% of 7th-9th grade students surveyed (n=10,154) reported using the Internet with no parental supervision. Another 36% indicated that they receive only "a little" parental supervision. Parental supervision at this age level is complicated by increasing privacy expectations of students, parents having more confidence in and expectations of their children, and adolescents assuming more mobile and socially interactive lifestyles. 55% of 7th-9th graders surveyed (n=10,366) reported that they commonly access the Internet from a private place in their home, and 44% (n=10,366) indicate that they commonly access the Internet from a private place in a friend's home. 30% (n=6,209) reported that their parents limit the amount of time they spend online.

Online risky behavior is also common with 42% of the students (n=9,631) within this grade cohort indicating that they have spoken with at least one online stranger within the past year. Probably due to the increased popularity of social networking sites, many students at this grade level are using the Internet to publicly post a variety of sensitive information including: photographs of themselves (39%, n=9,838); their real names (36%, n=9,809); schedules (14%, n=9,681); and personal contact information (14%, n=9,666) such as residential street address (7%, n=9,616). Additionally, 9% (n=9,486) of students surveyed reported they have accepted an invitation to meet someone online in-person and 10% (n=9,463) have asked someone online to meet in-person. (Note: question wording infers this to be a stranger, but this may not be strictly true for all survey responses. The large point is that many students are interacting online with people they know and likely do not know for any number of purposes.)

In contrast to the 4th-6th grade survey cohort, students at this level are nearly as likely to have experienced at least one form of computer abuse or crime asked about. Nearly 21% (n=9,899) have experienced one or more forms of deceit or abuse within the 2006-2007 school year. Cyber bullying was common within this grade cohort with 15% (n=9,998) reporting an embarrassing experience online and 13% (n=10,000) indicating that they had been bullied or threatened online.

Having another Internet user impersonate a student online was another common form of victimization (15%, n=10,009) along with unauthorized use of a password (15%, n=10,022). Sexual chat was reported to be much more common among 7th-9th grade students, with 14% (n=9,976) indicating that they had communicated with someone online about sexual things; 11% of students (n=9,989) reported that they had been asked to talk about sexual things online. Students within this grade cohort were also more likely to have been exposed to nude pictures of other Internet users (8%, n=9,987) and were also asked for nude pictures of themselves online (7%, n=9,989).

Students surveyed were asked to characterize the perpetrator of the forms of computer abuse they had experienced. As before, survey data reveal that students often know perpetrators beforehand. The most commonly chosen identifier was "a friend [they] know in person" (59%, n=5,023), and other identifiers that would indicate a prior relationship with a perpetrator such as "someone else [they] know" (36%, n=4,621) or a "classmate" (21%, n=4,640). Slightly fewer students indicated that online friends (19%, n=4,609) and online strangers (16%, n=4,576) were responsible for the incidents they experienced. Survey data also reveal that students are more likely to be victimized by other students rather than by adults, with selections of "girl" (46%, n=4,807) and "boy" (42%, n=4,812) perpetrators being more common than "woman" (12%, n=4,599) or "man" (11%, n=4,660).

It follows that students also indicated that they themselves are engaging in abusive behavior online. Indeed 53% of 7th-9th graders who participated in the survey (n=10,366) admitted they had engaged in at least one form of online deceit or abuse within the past school year. Lying about their age (24%, n=10,366) was the most common. Students at this age/grade level also commonly downloaded music they did not pay for (22%, n=10,366) and pretended to be someone else online (11%, n=10,366). Bullying and sexually related abuses were more common among students of this cohort, with 4% (n=10,366) admitting to embarrassing another person online, 4% (n=10,366) admitting to harassing or threatening another person online, 3% (n=10,366) admitting to asking for naked pictures from another Internet user and 3% (n=10,366) admitting to soliciting sexual chat online.

The 7th-9th grade cohort was also asked in the study if they circumvent existing security measures to access online content. 7% (n=10,366) of students reported they had done so within the school year. Academic dishonesty by using computers or electronic devices to cheat on assignments and tests was also somewhat common within this grade cohort, with 5% (n=10,366) admitting to online plagiarism, 5% (n=10,366) admitting to cheating on school work and 3% (n=10,366) admitting to cheating on tests.

Charts and tables of 7th-9th grade data are provided in Appendix M.

10th-12th Grade

Students at this grade level remembered beginning to use computers at eight years of age (n=7,133). On average, they report now using two separate devices to access the Internet with desktops (93%, n=7,334) and laptops (60%, n=7,334) being the most common. 28% (n=7,334) students indicated that they use a cell phone to access the Internet. Respondents most commonly indicated that they had learned the most about computers by being self-taught (36%, n=7,334), followed by being parent-taught (28%, n=7,334).

On average, students within this age/grade cohort level report that they spend a total of 21 hours per week engaged in various online activities (n=6,571). Approximately one in five students report that their parents limit the amount of time they spend on online in activities such as instant messaging (16% of respondents, n=7,122), text messaging (17%, n=7,081), social networking (14%, n=7,074) and web surfing (12%, n=7,054). Over a quarter of students surveyed (28%, n=5,645) indicated that family members or friends have suggested that they cut back on their Internet use.

Within the past year, many students in this grade cohort indicated that they have used the Internet to interact with strangers online in a variety of ways, including: chatting (48%, n=5,358); flirting (25%, n=5,304); providing personal information (22%, n=5,313); talking about private things (17%, n=5,321) and engaging in sexually oriented chat (15%, n=5,303). Survey data also reveal that students are using the Internet to meet online strangers in-person; 14% (n=5,312) have accepted an invitation to meet an online stranger in-person; 14% of students (n=5,302) have invited an online stranger to meet them in-person.

Within the past school year, 41% (n=7,030) students reported that they had experienced at least one form of computer-related abuse, and more than 26% (n=6,997) revealed they had experienced two or more forms of computer abuse. The most commonly reported forms of victimization were malware attacks (40%, n=7,030) and denial of service attacks (36%, n=6,993) that may be periodically experienced by all members of society who use the Internet. However, many students also report having experienced cyber bullying within the past school year (16%, n=6,967), having been embarrassed online (16%, n=6,974), harassed online (17%, n=6,963), and stalked online (15%, n=6,983). Approximately one in four students at this age/grade level reported they had been exposed to unwanted pornography online (23%, n=6,959) or asked about sexual things online (23%, n=6,950).

When asked to characterize the perpetrator(s) responsible students primarily indicated that the perpetrator was a "boy or man" (35%, n=3,768). Of those who could identify the perpetrator most indicated the person was a "friend" (34%, n=3,683) followed by "girl or woman" (30%, n=3,600) and "classmate" (23%, n=3,591). These data underscore the reality that a substantial amount of online victimization experienced by youth stem from the behaviors of their peers rather than adult strangers. Indeed, the majority of students (75%, n=4,455) within this grade cohort admit to having engaged in some form of abusive behavior online within the past year. Half of the students surveyed (51%, n=4,396) reported having committed three or more forms of deceitful, abusive, questionable and/or criminal behaviors asked about (see Appendix E, Questions 27-33).

The most commonly reported behavior was lying about one's age online (30%, n=6,723). Cheating and plagiarism were also commonly reported. 21% of students (n=6,697) revealed they used a computer or electronic device to cheat

on a school assignment, 12% (n=6,690) committed plagiarism and 9% (n=6,684) reported having used a computer or electronic device to cheat on an exam.

Within the past year 65% (n=6,810 students) have illegally downloaded music, 34% (n=6,620) have illegally downloaded movies and 30% (n=6,573) have illegally downloaded software. Students are aware of and circumventing security systems designed to prevent them from accessing Internet content (12%, n=6,575). Fewer students within this grade cohort are engaged in cyber bullying activities with 9% (n=6,662) having admitted to harassing someone online and 8% (n=6,664) having admitted to threatening someone online within the school year.

Charts and tables of 10^{th}-12^{th} grade data are provided in Appendix N.

CONCLUSIONS AND RECOMMENDATIONS

The *RIT Survey of Internet and At-risk Behaviors* conducted in Monroe County school districts from spring 2007 through January 2008 involved 40,079 K-12th grade students along with hundreds of school staff members and parents. Survey results confirm that students begin using the Internet at very young ages. When they do many students of all grade levels use personal computers from home and other locations, and from relatively public or private places, to access various online content for different reasons. Older students also routinely use cell phones and other mobile devices to access Internet content in the course of playing games, interacting with friends and doing school work, among other activities. This is often accomplished without close supervision or positive role modeling by parents or other respected adults especially as children get older. Although students report learning about computers from their parents, many report being self-taught. Having not grown up using computers, many parents and teachers report believing that today's youth know more about using computer technology than they do.

Indeed, K-12^{th} grade students are increasingly using computers, other electronic devices and the Internet at younger ages — this technology is now integral to their lives. On balance computing is probably good for students, families, communities and all of society. However, in the absence of needed supervision, role modeling and systematically delivered education in how to be safe, secure and ethical online, today's youth including Monroe County school district students are apt to experience inappropriate content and online victimization. It is also true that certain proportions of Monroe County school district students commit various forms of deceit, abuse and/or crime online including, but not limited to, academic dishonesty, cyber bullying and pirating of music, movies and software. Many adolescent students who are naturally exploring sexuality use the Internet to access and communicate sex-related content.

These and other behaviors, and issues pertaining to online technology and content, represent new educational challenges for school districts everywhere. Chief among policy questions that need to be addressed by school administrators, staff, parents and elected officials are:

1. What Internet safety, information security and/or cyber ethics instruction (if any) should the district provide to students?

2. What specific topics should be addressed, for grades K-12?

3. Into what courses or aspects of curricula could such instruction be logically incorporated; and how would this map to state and national education standards (e.g., for technology, health and safety, etc.)?

4. Through what pedagogical methods would cyber-related instruction be most effectively taught to promote student learning and knowledge retention and bring about positive behavioral changes?

5. What resources already exist that could be adopted in whole or in part to facilitate the District's educational offerings in this area?

6. What role can/should parents have in supporting implementation of cyberrelated instruction beyond what is currently being offered by the District, and how might this be accomplished?

By participating in the *RIT Survey of Internet and At-risk Behaviors* Monroe County school districts are already positioned to begin answering these questions. In August – October of 2007, Fairport Central School District pioneered a *Cyber Leadership Institute* to begin exploring these and related questions. The Institute consisted of five days of intensive workshops attended by key personnel. Results of that district's participation in this survey were used to inform staff discussions and preliminary recommendations for moving the FCSD forward toward implementing cyber safety, security and ethics education. Perhaps a similar staff/policy development effort could be undertaken in other Monroe County districts.

The Cyber Safety and Ethics Initiative, as it is now known (www.bcybersafe.org) is currently working to provide such opportunities for area school districts, including Monroe County school districts. This report underscores the need to do so sooner than later and in a fairly comprehensive and structured manner that takes into account staff development, technology procurement and policy, and the digital youth culture of modern society.

EXHIBIT B

iKeepSafe C3 MATRIX™ DIGITAL CITIZENSHIP

A Companion to the Augmented Technology Literacy Standards for Students

INTRODUCTION

The iKeepSafe Digital Citizenship C3 Matrix™ is designed to assist educators in integrating the concepts of cyber-safety, cyber-security, and cyber-ethics (C3) into existing technology and literacy standards and curricula. Based on the C3 Framework created by education and technology expert Davina Pruitt-Mentle, Ph.D., the C3 Matrix takes a holistic and comprehensive approach to preparing students for 21st century digital communication. Competency levels for C3 concepts are divided into three levels: basic, intermediate, and proficient.

Cyber-safety, Cyber-security, Cyber-ethics, (C3) Digital Literacy Skills

The vision guiding the iKeepSafe Digital Citizenship C3 Matrix springs from the vision of Eleanor Roosevelt and the ancient Greeks that the true purpose of education is to produce citizens. All students must have the awareness, knowledge, opportunity and resources to develop the C3 skills required for full participation as informed, responsible, ethical and productive citizens. The C3 Matrix provides educators with guidance regarding cyber-safety, security, and ethics principles that all students should know and be able to apply independently when using technology, technology systems, digital media and information technology, including the Internet.

Although C3 concepts are presented here as separate categories, they are not distinct and/or separable; they are, in fact, interrelated and should be considered as a whole. These principles should be embedded systemically throughout students' K-12 experience, not taught in isolation, and should be applied when meeting learning outcomes in the content areas. They can also be used as a companion and supplement to the various technology literacy standards for students created by ISTE, AASL, AECT, and others.

The three competency levels outlined in the C3 Matrix are not identified by grade level; rather, they represent progressive levels of cognitive complexity at which youth should be expected to understand and practice. The levels were developed utilizing Bloom's *Taxonomy of Educational Objectives* (2001 revised edition), a hierarchy of six progressively complex cognitive processes that learners use to attain objectives or perform activities. Bloom's Taxonomy, the preferred system for articulating program objectives, categorizes cognitive skills by increasing order of complexity. From least to most complex these are: remembering, understanding, applying, analyzing, evaluating, implementing, and creating.

This taxonomy aids curriculum developers, policy makers and instructional designers in better defining the desired learning level of a target audience and then developing an appropriate design that will help the learner achieve desired learning goals. Additionally, this taxonomy aids in crafting behavioral assessment instruments.

What follows is a theoretical framework that can be used to inform a national, regional, or local agenda. It uses three dimensions, based on practical circumstances and experiences with educating students and teachers, with

Anderson, L. W., & Krathwohl, D. R. (Eds.). (2001). A taxonomy for learning, teaching and assessing: A revision of Bloom's Taxonomy of educational objectives: Complete edition. New York : Longman.

input from multiple stakeholders including parents, students, educators, technology coordinators, media specialists, curriculum resource teachers, Internet safety experts, and industry security specialists. While C3 subject areas have common ground, they also have significant content that is distinct and important in discussing on an individual basis.

Cyber-safety

Cyber-safety addresses the ability to act in a safe and responsible manner on the Internet and other connected environments. These behaviors protect personal information and reputation and include safe practices to minimize danger from behavioral-based, rather than hardware/software-based, problems.

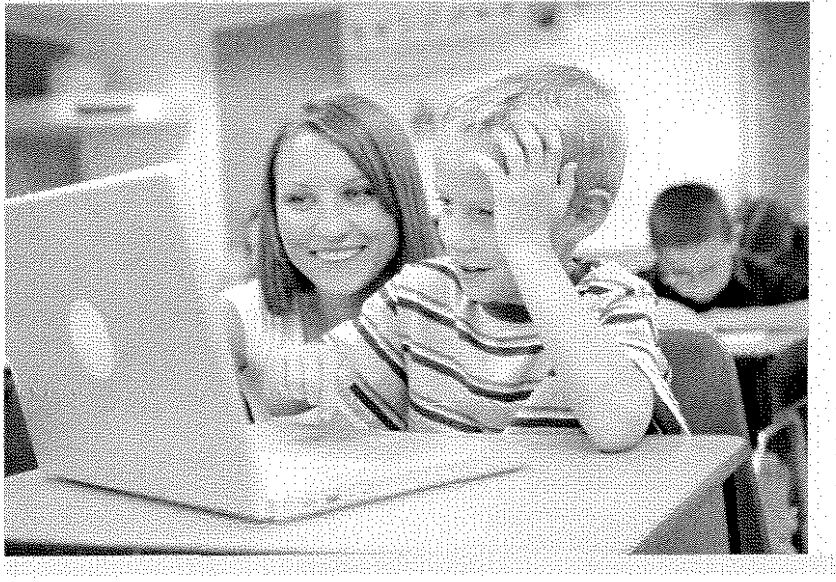
Cyber-security

Whereas cyber-safety focuses on acting safely and responsibly, cyber-security covers physical protection (both hardware and software) of personal information and technology resources from unauthorized access gained via technological means. Cyber-security is defined by HR 4246, Cyber Security Information Act (2000) as "the vulnerability of any computing system, software program, or critical infrastructure to, or their ability to resist, intentional interference, compromise, or incapacitation through the misuse of, or by unauthorized means of the Internet, public or private telecommunications systems, or other similar conduct that violates federal, state, or international law, that harms interstate commerce of the US, or that threatens public health or safety." In contrast, most of the issues covered in cyber-safety are steps that one can take to avoid revealing information by "social" means.

Cyber-ethics

Cyber-ethics is the discipline of using appropriate and ethical behaviors and acknowledging moral duties and obligations pertaining to online environments and digital media.

Cyber-safety, security, and ethics cannot be stagnant, because technologies are dynamic and ever changing. For example, cyber-ethical issues are experiencing vast transformation as a result of factors driven by the multi-media aspects of cell phones and the immense reservoir of information on the Internet. It is essential that educators have tools for technology education that are also dynamic and evolving. The C3 Matrix provides these tools for teachers and administrators—and the students they teach.



cable in the classroom
Kids. Cable. Learning.

cmch
center on media and child health

PENNSTATE

HARVARD SCHOOL OF PUBLIC HEALTH

Virginia Department of Education

CoSN
ADVANCING K-12 TECHNOLOGY LEADERSHIP

STAYSAFEONLINE.org
National Cyber Security Alliance

R·I·T

Florida Gulf Coast University

The iSchool at Drexel

SETDA

C3 Framework
Promoting Responsible Use

I. Cyber-Ethics

Students recognize and practice responsible and appropriate use while accessing, using, collaborating, and creating technology, technology systems, digital media and information technology. Students demonstrate an understanding of current ethical and legal standards, the rights and restrictions that govern technology, technology systems, digital media and information technology within the context of today's society. Students will:

A. Understand and follow acceptable polices (school, home and community), and understand the personal and societal consequences of inappropriate use.
B. Demonstrate and advocate for ethical and legal behaviors among peers, family, and community.
C. Practice citing sources of text and digital information and make informed decisions about the most appropriate methods for avoiding plagiarism.
D. Make ethical and legal decisions while using technology, technology systems, digital media and information technology when confronted with usage dilemmas.
E. Exhibit responsibility and Netiquette when communicating digitally.
F. Recognize the signs and emotional effects, the legal consequences and effective solutions for Cyberbullying.
G. Recognize appropriate time and place to use digital tools, techniques and resources.
H. Understand the importance of online identity management and monitoring. Advocate others to understand the importance of Online Reputation Management.

II. Cyber-Safety

Students practice safe strategies to protect themselves and promote positive physical and psychological well-being when using technology, technology systems, digital media and information technology including the Internet. Students will:

A. Recognize online risks, to make informed decisions, and take appropriate actions to protect themselves while using technology, technology systems, digital media and information technology.
B. Make informed decisions about appropriate protection methods and safe practices within a variety of situations.
C. Demonstrate and advocate for safe behaviors among peers, family, and community.

III. Cyber-Security

Students practice secure strategies when using technology, technology systems, digital media and information technology that assure personal protection and help defend network security. Students will:

A. Recognize online risks, make informed decisions, and take appropriate actions to protect themselves while using technology, technology systems, digital media and information technology.
B. Make informed decisions about appropriate protection methods and secure practices within a variety of situations.
C. Demonstrate commitment to stay current on security issues, software and effective security practices.
D. Advocate for secure practices and behaviors among peers, family, and community.

CYBER-SAFETY

iKeepSafe C3MATRIX DIGITAL CITIZENSHIP

Physical and Psychological Well-being:

Students practice safe strategies to protect themselves and promote positive physical and psychological well-being when using technology, technology systems, digital media and information technology, including the Internet.

	BASIC	INTERMEDIATE	PROFICIENT
A. Recognize online risks, make informed decisions, and take appropriate actions to protect themselves while using technology, technology systems, digital media and information technology.	**Safe and Responsible Practices** • **Recognize** safety issues* related to technology, technology systems, digital media and information technology including the Internet (e.g., online predator tactics, posting controversial content). • **Use** safe practices related to technology, technology systems, digital media and information technology including the Internet. • **Recognize** and **understand** the purpose of protection measures (including filtering systems) for various types of technology, technology systems, digital media and information technology.	**Safe and Responsible Practices** • **Recognize** and **discuss** safety issues related to technology, technology systems, digital media and information technology including the Internet (e.g., online predator tactics, posting controversial content). • **Use** safe practices and procedures related to technology, technology systems, digital media and information technology including the Internet. • **Explain** the purpose of technology, technology systems, digital media and information technology protection measures.	**Safe and Responsible Practices** • **Recognize** and **discuss** safety issues related to technology, technology systems, digital media and information technology including the Internet (e.g., online predator tactics, posting controversial content). • **Use** safe practices and procedures related to technology, technology systems, digital media and information technology including the Internet. • **Explain** the purpose of and analyze the use of different protection measures for technology, technology systems, digital media and information technology.
B. Make informed decisions about appropriate protection methods and secure practices within a variety of situations.	• **Adhere** to privacy and safety guidelines, policies, and procedures. • **Discuss** the potential for addictive behaviors and the excessive use of technology and Internet. • **Describe** procedures for exiting an inappropriate site. • **Describe** procedures for reducing the chance of being a victim of cyber-bullying. • **Describe** procedures for reporting cyber-bullying and other inappropriate behavior or content.	• **Adhere** to privacy and safety guidelines, policies, and procedures. • **Describe** technology and Internet addictive behaviors. • **Describe** procedures for exiting an inappropriate site. • **Describe** procedures for reducing the chance of being a victim of cyber-bullying. • **Describe** effective steps to manage and resolve a cyber-bullying situation. • **Model** understanding about current safety needs.	• **Adhere** to privacy and safety guidelines, policies, and procedures. • **Describe** and **practice** procedures for disciplined and productive Internet use (e.g., balance between time on and off the Internet). • **Describe** and **practice** procedures for exiting an inappropriate site. • **Describe** and **practice** procedures for reducing the chance of being a victim of cyber-bullying. • **Describe** and **practice** effective steps to manage and resolve a cyber-bullying situation.
C. Demonstrate and advocate for safe behaviors among peers, family, and community.		• **Model** personal safety within a variety of situations.	• **Model** personal safety within a variety of situations. • **Demonstrate** commitment to stay current on safety issues and effective protection practices. • **Advocate** for safe practices and behaviors among peers, family, and community.

* Safety issues could include but are not limited to: upload and download of objectionable content, cyber-bullying, reputation damage, response to unwanted communications from businesses or predators, and Internet addiction.

CYBER-SECURITY

iKeepSafe C3 MATRIX DIGITAL CITIZENSHIP

Digital Security:

Practice secure strategies that assure personal protection and help defend network security.

	BASIC	INTERMEDIATE	PROFICIENT
A. Recognize security risks, make informed decisions, and take appropriate actions to protect themselves while using technology, technology systems, digital media and information technology.	**Secure Practices** • **Understand** security risks and the potential harm of intrusive applications related to technology, technology systems, digital media, and information technology including the Internet (e.g. email viruses, digital propaganda, spy ware, adware, identity theft, phishing/pharming/spoofing scams, spam, social engineering). • **Understand** effective basic security practices related to technology, technology systems, digital media and information technology including the Internet (e.g., strong passwords, protecting password and user ID, not disclosing important personal information, minimizing/evaluating pop up ads). • **Recognize** and **understand** the purpose of technology, technology systems, digital media and information technology security protection measures. • **Discuss** strategies for managing everyday hardware and software problems.	**Secure Practices** • **Understand** and **discuss** security risks and the potential harm of intrusive applications related to technology, technology systems, digital media and information technology including the Internet (e.g. email viruses, digital propaganda, spy ware, adware, identity theft, phishing/pharming/spoofing scams, spam, social engineering). • **Describe** and **practice** effective security practices, beyond the basic level, related to technology, technology systems, digital media and information technology including the Internet. • **Recognize** and **understand** the purpose of security protection measures for technology, technology systems, digital media and information technology. • **Model** understanding about current security needs.	**Secure Practices** • **Understand** and **discuss** security risks and the potential harm of intrusive applications related to technology, technology systems, digital media and information technology including the Internet (e.g. email viruses, digital propaganda, spy ware, adware, identity theft, phishing/pharming/spoofing scams, spam, social engineering). • **Practice** effective security practices and **analyze** new options, beyond the intermediate level, related to technology, technology systems, digital media and information technology including the Internet and **critically evaluate** digital resources. • **Recognize** and **understand** the purpose of security protection measures for technology, technology systems, digital media and information technology.
B. Make informed decisions about appropriate protection methods and secure practices within a variety of situations.		• **Adhere** to security guidelines, policies, and procedures. • **Use effective** strategies for managing everyday hardware and software problems. • **Use effective** strategies for securing wireless connections (e.g., connecy to only legitimate wi-fi hot spots or turn off wi-fi, turn off file share mode, encrypt sensitive data/ information, use and update anti-virus software, use a firewall, update operating system).	• **Adhere** to security guidelines, policies, and procedures. • **Describe** and **practice** strategies for managing everyday hardware and software problems. • **Describe** and **practice** strategies for securing wireless connections (e.g., connect to only legitimate wi-fi hot spots or turn off wi-fi, turn off file share mode, encrypt sensitive data/ information, use and update anti-virus software, use a firewall, update operating system.
C. Demonstrate commitment to stay current on security issues, software and effective security practices.		• **Model** secure practices within a variety of digital communities.	• **Model** secure practices within a variety of digital communities.
D. Advocate for secure practices and behaviors among peers, family, and community.			• **Advocate** for secure practices and behaviors among peers, family, and community.

CYBER-ETHICS

iKeepSafe C3MATRIX DIGITAL CITIZENSHIP

Legal and Ethical Issues:

Students recognize and practice responsible and appropriate use while accessing, using, collaborating, and creating technology, technology systems, digital media and information technology. Students demonstrate an understanding of current ethical and legal standards, rights and restrictions governing technology, technology systems, digital media and information technology within the context of today's society.

	BASIC	INTERMEDIATE	PROFICIENT
A. Understand and follow acceptable use polices (school, home and community), and understand the personal and societal consequences of inappropriate use.	• **Understand** and **follow** acceptable use policies (e.g., school, home, and community settings). • **Discuss** basic issues related to responsible use of technology, technology systems, digital media and information technology, and **describe** personal consequences of inappropriate use*.	• **Understand** and **follow** acceptable use policies (e.g., school, home, and community settings). • **Demonstrate** responsible use of technology, technology systems, digital media and information technology in different settings (e.g., school, home, and community settings) and **describe** and **analyze** personal and societal consequences of inappropriate use.	• **Understand** and **follow** acceptable use policies (e.g., school, home, and community settings). • **Demonstrate** responsible use of technology, technology systems, digital media and information technology in different settings (e.g., school, home, and community) and **describe** and **analyze** personal and societal consequences of inappropriate use. • **Make informed choices** about acceptable use of technology, technology systems, digital media and information technology when confronted with usage dilemmas.
B. Demonstrate and advocate for ethical and legal behaviors among peers, family, and community.			• **Demonstrate** and **advocate** for legal and ethical behaviors among peers, family, and community regarding responsible use of technology, technology systems, digital media and information technology.
C. Practice citing sources of text and digital information and make informed decisions about the most appropriate methods for avoiding plagiarism.	• **Understand** and **follow** ethical standards of conduct (e.g., AUP, Student Handbooks, Student Code of Conduct, Honor Codes). • **Discuss** definitions and basic concepts and issues related to plagiarism/electronic cheating and **describe** personal and societal consequences of plagiarism. • **Demonstrate** appropriate strategies for avoiding plagiarism (e.g., quoting, citing, acknowledging source and/or paraphrasing). **Discuss** the importance of respecting the rights of others regarding their work.	• **Understand** and **follow** ethical standards of conduct (e.g., AUP, Student Handbooks, Student Code of Conduct, Honor Codes). • **Discuss** definitions and basic concepts and issues related to plagiarism/electronic cheating and **describe** personal and societal consequences of plagiarism. • **Practice** citing sources of text and digital information. **Determine** and **practice the use of** appropriate strategies for avoiding plagiarism (e.g., quoting, citing, acknowledging source and/or paraphrasing).	• **Understand** and **follow** ethical standards of conduct (e.g., AUP, Student Handbooks, Student Code of Conduct, Honor Codes). • **Discuss** definitions and basic concepts and issues related to plagiarism/electronic cheating and **describe** personal and societal consequences of plagiarism. • **Demonstrate** appropriate strategies for avoiding plagiarism (e.g., quoting, citing, acknowledging source and/or paraphrasing) • **Determine** the most appropriate method for avoiding plagiarism and **create** original work and **practice** citing sources of text and digital information. • **Demonstrate** and **advocate** for ethical behaviors among peers, family, and community.

* Inappropriate use could include, but is not limited to, viewing inappropriate content, using the school's network for non-educational purposes, or work networks for non-school/work related activities, posting incorrect/inaccurate information, bullying, participating in hate groups, harassing or sending/posting mean comments, hacking, illegally downloading copyrighted materials/movies/music and/or making and sharing copies of copyrighted materials, etc..

CYBER-ETHICS

	BASIC	INTERMEDIATE	PROFICIENT
D. Make ethical and legal decisions when confronted with usage dilemmas while using technology, technology systems, digital media and information technology.	• **Discuss** definitions and basic concepts and issues related to intellectual property, media copyright laws, private/public domain, fair use and file sharing. • **Describe** personal and societal consequences of respecting verses ignoring rights, laws and practices such as copyright, private/public domain, fair use and file sharing. • **Understand** and **follow** school, home and community policies on access to information resources.	• **Discuss** definitions and basic concepts and issues related to intellectual property, media copyright laws, private/public domain, fair use, and file sharing. • **Describe** personal and societal consequences of respecting verses ignoring rights, laws and practices such as copyright, private/public domain, fair use and file sharing. • **Understand** and **follow** school, home and community policies on access to information resources and adhere to local, state, and federal laws. • **Demonstrate** appropriate social and ethical behaviors when using technology and digital media including the recognition of intellectual property rights, fair use of copyrighted material, and legal file sharing or downloading of software, music and videos. • **Make ethical and legal use** of technology, technology systems, digital media and information technology when confronted with usage dilemmas.	• **Discuss** definitions and basic concepts and issues related to intellectual property, media copyright laws, private/public domain, fair use, and file sharing. • **Describe** personal and societal consequences of respecting verses ignoring rights, laws and practices such as copyright, private/public domain, fair use, and file sharing. • **Describe** personal and societal consequences involving intellectual property rights, media copyright laws, private/public domain, fair use, and file sharing. • **Understand** and **follow** school, home and community policies on access to information resources and adhere to local, state, and federal laws. • **Distinguish** the legal implications between personal, educational, and commercial uses of protected works. • **Demonstrate** social and ethical behaviors when using technology and digital media regarding intellectual property recognition, fair use of copyrighted material, including file-sharing and pirating versus legal downloading of software, music and videos. • **Make ethical and legal use** of technology, technology systems, digital media and information technology when confronted with usage dilemmas. • **Demonstrate** and **advocate** for legal and ethical behaviors in this domain among peers, family, and community.
E. Exhibit responsibility and netiquette (i.e appropriate digital communication skills) when communicating digitally.	• **Recognize** personal differences and **practice** etiquette within diverse situations. • **Recognize** positive and negative social and ethical behaviors when using technology and digital media and information technology.	• **Recognize** personal differences and practice etiquette within diverse digital communities. • **Recognize** positive and negative social and ethical behaviors when using technology and digital media and information technology.	• **Recognize** personal differences and practice etiquette within diverse digital communities. • **Recognize** and **analyze** positive and negative social and ethical behaviors when using technology and digital media and information technology.

CYBER-ETHICS

	BASIC	INTERMEDIATE	PROFICIENT
F. Recognize the signs, emotional effects, legal consequences of and effective solutions for cyber-bullying.	• **Understand** and **discuss** the signs and solutions for cyber-bullying. • **Recognize** appropriate time and place to use digital tools, techniques, and resources (e.g., when appropriate to use lingo and emoticons, when to use cell phone and text message). • **Apply** proper communication skills when communicating digitally.	• **Demonstrate** a thorough understanding of the signs, emotional effects, legal consequences of, and effective solutions for cyber-bullying. • **Recognize** appropriate time and place to use digital tools, techniques, and resources (e.g., when appropriate to use lingo and emoticons, when to use cell phone and text message).	• **Demonstrate** a thorough understanding of the signs, emotional effects, legal consequences of, and effective solutions for cyber-bullying. • **Make informed choices** when confronted with cyber-bullying dilemmas. • **Recognize** appropriate time and place to use digital tools, techniques and resources (e.g., when appropriate to use lingo and emoticons, when to use cell phone and text message). • **Apply** appropriate communication skills when communicating digitally. • **Practice** digital etiquette to support collaboration • **Advocate** for proper netiquette behaviors among peers, family, and community.
G. Recognize appropriate time and place to use digital tools, techniques and resources.	• **Understand** that content posted to the web or sent through other digital means (e.g., cell phones, cameras) is accessible to a wide audience and can be permanently archived.	• **Understand** that content posted to the web or sent through other digital means (e.g., cell phones, cameras) is accessible to a wide audience and can be permanently archived.	• **Understand** that content posted to the web or sent through other digital means (e.g., cell phones, cameras) are accessible to a wide audience and can be permanently archived.
H. Understand the importance of online identity management and monitoring (ORM). Advocate others to understand the importance ORM.	• **Understand** the importance of online reputation management and monitoring (ORM). • **Recognize** positive and negative uses of electronic postings as related to ORM	• **Understand** the importance of online reputation management and monitoring (ORM). • **Recognize** positive and negative uses of electronic postings as related to ORM. • **Demonstrate** appropriate strategies for protecting, monitoring and/or positively promoting personal identity- Online Reputation Management and monitoring (ORM).	• **Understand** the importance of online reputation management and monitoring (ORM). • **Recognize** positive and negative uses of electronic media/postings as related to ORM. • **Demonstrate** appropriate strategies for protecting, monitoring, and/or positively promoting personal identity (i.e. ORM). • **Analyze** selected electronic media/postings and reflect, as an individual, on the appropriateness of each for effective ORM.

A U G M E N T E D

Technology Literacy Standards for Students

This graph is designed to help educators see how C3 concepts (cyber-safety, cyber-security, and cyber-ethics) can be integrated into existing standards. A teacher or technology coordinator may refer back to the C3 Matrix for ways to address safety, security, and ethics while teaching concepts from the national standards.

How content addresses:

- ISTE/NETS•S Standards
- **AASL Standards for the 21st Century Learner**
- AASL/AECT Information Literacy Standards for Student Learning
- **iKeepSafe Digital Citizenship C3 Matrix**
- *21st Century Framework*

Activity/Module:

* Completion of any activity does not certify competency in the identified area; however, it will contribute to development of the competency

ISTE/NETS•S Standard and Outcomes	Indicators	Addressed in this activity	EXAMPLE
1. Creativity & Innovation Students demonstrate creative thinking, construct knowledge, and develop innovative products & processes **AASL 1.1.1, 1.2.1, 1.2.3., 2.1.1., 2.1.6., 2.2.4., 4.1.5., 4.1.8.** AASL/AECT 1.3, 3.2, 3.3, 5.3, iKeepSafe C3 Matrix 21st 1.1, 1.4, 2.4, 2.5, 3.1,	**Students:** **a.** apply existing knowledge to generate new ideas, products, or processes **b.** create original works as a means of personal or group expression **c.** use models and simulations to explore complex systems and issues **d.** identify trends and forecast possibilities.	☐ **Yes** ☐ **No**	
2. Communication and Collaboration Students use digital media and environments to communicate and work collaboratively, including at a distance, to support individual learning and contribute to the learning of others. **AASL 1.1.9., 1.3.2., 1.3.4., 2.1.4., 2.1.5., 2.2.4., 2.3.2., 3.1.1.,3.1.2., 3.1.4., 3.2.1., 3.2.3., 3.3.1., 3.3.2.,3.4.3.,4.2.1.,4.3.1.,4.4.4.** AASL/AECT 3.4, 5.3, 9.1, 9.2, 9.3, 9.4, 7.1, C3 Conceptual Framework 21st 1.2, 1.3, 3.1, 4.1, 4.2, 4.3,8.1, 8.2,10.1, 10.2, 10.3,	**Students**: a. interact, collaborate, and publish with peers, experts, or others employing a variety of digital environments and media. b. communicate information and ideas effectively to multiple audiences using a variety of media and formats. c. develop cultural understanding and global awareness by engaging with learners of other cultures. d. contribute to project teams to produce original works or solve problems.	☐ **Yes** ☐ **No**	
3. Research and Information Fluency Students apply digital tools to gather, evaluate, and use information **AASL 1.1.4, 1.1.5, 1.1.6., 1.1.7, 2.1.1., 2.1.2., 2.2.3., 2.2.4., 3.1.1.,3.1.4., 3.4.2., 4.1.6.** AASL/AECT 1.2, 1.4,1.5, 2.1, 2.2, 2.3, 2.4, 3.1, 4.1, 4.2, 6.1, iKeepSafe C3 Matrix 21st 2.4, 2.5, 5.1, 5.2, 6.3, 7.1, 7.2, 11.2, 12.3	**Students:** **a.** plan strategies to guide inquiry. **b.** locate, organize, analyze, evaluate, synthesize, and ethically use information from a variety of sources and media. **c.** evaluate and select information sources and digital tools based on the appropriateness to specific tasks. **d.** process data and report results.	☐ **Yes** ☐ **No**	

4. Critical Thinking, Problem Solving and Decision Making Students use critical thinking skills to plan & conduct research, manage projects, solve problems, and make informed decisions using appropriate digital tools & resources **AASL 1.1.1, 1.1.3, 1.1.4., 1.2.2., 1.2.4.,1.3.2., 2.1.3.,3.1.4., 3.2.3., 3.3.4., 4.2.3.** AASL/AECT 6.2, iKeepSafe C3 Matrix 21st 2.1, 2.2,2.4, 3.5,4.1, 4.2,8.1, 8.2, 9.4, 9.5,	**Students:** a. identify and define authentic problems and significant questions for investigation. b. plan and manage activities to develop a solution or complete a project. c. collect and analyze data to identify solutions and/or make informed decisions. d. use multiple processes and diverse perspectives to explore alternative solutions.	☐ Yes ☐ No	
5. Digital Citizenship Students understand human, cultural, and social issues related to technology & practice legal and ethical behavior **AASL 1.3.1., 1.3.3., 1.3.5., 2.3.3., 3.1.6., 3.2.2.,3.3.7.,4.3.4., 4.4.3., 4.4.4., 4.4.5.** AASL/AECT 8.1, 8.2, 8.3, 7.1, C3 Conceptual Framework 21st 4.1, 4.2, 4.3, 5.2, 6.2, 6.3, 7.2, 9.6, 10.1, 10.2, 10.3, 12.3	**Students:** a. advocate and practice safe, legal, and responsible use of information and technology. b. exhibit a positive attitude toward using technology that supports collaboration, learning, and productivity. c. demonstrate personal responsibility for lifelong learning. d. exhibit leadership for digital citizenship.	☐ Yes ☐ No	
6. Technology Operations & Concepts Students demonstrate a sound understanding of technology concepts, systems, and operations **AASL 1.1.8., 2.1.4., 3.4.2.** C3 Conceptual Framework	**Students:** a. understand and use technology systems. b. select and use applications effectively and productively. c. troubleshoot systems and applications. d. transfer current knowledge to learning of new technologies.	☐ Yes ☐ No	

Correlation of the ISTE/NET•S & AASL/AECT, 21st Century Framework and C3 Matrix

AASL Addressed				AASL/AECT Addressed										C3 Matrix	21st Century Framework Addressed											
1	2	3	4	1	2	3	4	5	6	7	8	9	ISTE/NETS*S Standards	Cyberethics Cybersafety Cybersecurity	1	2	3	4	5	6	7	8	9	10	11	12
X	X		X	X		X		X	X	X			1. Creativity & Innovation	X	X	X	X										
X	X	X	X			X		X		X		X	2. Communication & Collaboration	X	X		X	X				X		X			
X	X	X	X	X	X	X	X		X				3. Research & Information Fluency	X		X			X	X	X					X	
X	X	X							X				4. Critical Thinking, Problem Solving and Decision Making	X		X		X				X	X				
X	X	X	X							X	X		5. Digital Citizenship	X				X	X	X	X		X	X			X
		X											6. Technology Operations & Concepts	X													

NETS•S -Educational Technology Standards and Performance Indicators for Students: http://www.iste.org/Content/NavigationMenu/NETS/ForStudents/2007Standards/NETS_for_Students_2007.htm
AASL - http://www.ala.org/ala/mgrps/divs/aasl/aaslproftools/learningstandards/standards.cfm
AASL/AECT - http://www.ala.org/ala/mgrps/divs/aasl/aaslprotools/informationpower/InformationLiteracyStandards_final.pdf
Partnership for 21st Century Skills http://www.21stcenturyskills.org/index.php?itemid=120&id=254&option=com_content&task=view
Numerical ordering of skill/definitions are assigned for brevity within table format.

EXHIBIT C

Recommendations for Digital Citizenship Standards, by concept and grade level. Concepts are differentiated by media literacy, online behavior, safety, and security.

Digital Media Literacy

Digital media literacy is the ability to access, understand and participate in or create content by using digital media.

Developments in digital technology have had significant effects on the way individuals interact with communications and media services. An increasingly wide range of sources of information, ways of doing business, services (including government services) and entertainment are now commonly made available and accessed online and/or through digital media.

Positive Online Behavior

Positive online behavior is the ability to develop positive, appropriate and constructive online relationships with peers, family and strangers in a variety of mediums.

Key concepts associated with positive online behavior include netiquette, appropriate contact and communication with others, and consideration of issues such as cyber-bullying, problematic usage and unethical behavior.

Peer and Personal Safety

Peer and personal safety involves developing protective behaviors while using a range of online mediums including social networking and blogging. These behaviors include protecting personal information to safeguard privacy, identifying when feeling unsafe and recognizing grooming tactics.

Personal information is any information or combination of information that enables the identification of an individual.

Personal information may include full name and address details, phone numbers, email addresses, user names and passwords, bank details, and student identity card or passport details.

The role of the trusted adult is central to maintaining personal safety, while adopting appropriate behaviors towards others is central to ensuring peer safety. For older students, the concept of the digital footprint is explored. Educators should note that the students in

their classrooms who are most at risk for self-destructive behaviors (e.g., drug and alcohol abuse, suicide, eating disorders) are also most at risk for Internet threats.

e-Security

e-Security is the process of ensuring that electronic information is kept safe from corruption and malicious attack, and that access to it is suitably and effectively controlled.

Good e-security practice involves implementing e-security measures such as installing protective software.

The focus of this capability is understanding basic computer protection and the consequences of not protecting computers and files.

The skills, knowledge and behaviors required to protect personal information online are covered in the peer and personal safety capability.

Grade Levels	Digital Media Literacy	Positive Online Behavior	Peer and Personal Safety	e-Security
	Digital Media Literacy is the ability to access, understand and participate in or create content by using digital media.	Positive online behavior is the ability to develop positive, appropriate and constructive online relationships with peers, family and strangers in a variety of mediums.	Peer and personal safety involves developing protective behaviors while using a range of online mediums including social networking. Behaviors include protecting personal information to safeguard privacy, identifying when feeling unsafe and recognizing grooming tactics.	e-Security is the process of ensuring that electronic information and the hardware that stores it is kept safe from corruption and malicious attack, and that access to it is suitably and effectively controlled.
K-1	**K-1 student proficiency may include:** • understanding protocols of digital communications devices with supervision and may use: • the phone/mobile • email[1]	**K-1 student proficiency may include:** • developing an understanding of cyberspace as a community of real people • learning about the social conventions in the real world and cyberspace	**K-1 student proficiency may include:** • demonstrating an understanding that children need adult assistance when exploring cyberspace • differentiating between public information and personal	**K-1 student proficiency may include:** • exploring email for communication with family and friends • understanding basic security practices (e.g., strong passwords, protecting

[1] General instruction in email use is ***not*** recommended for first grade students as they are not prepared to understand all the relevant safety issues. However, in populations where email use has already begun by first grade, safety instruction should be offered, including: protecting email addresses (not posting to websites), avoiding contact with online strangers through email, phishing scams, malware downloads, and viruses.

Grade Levels	Digital Media Literacy	Positive Online Behavior	Peer and Personal Safety	e-Security
	• selected internet sites • the School Intranet • identifying and differentiating between online and offline content • searching for and viewing age-appropriate digital content; for example, student- or family-friendly websites.	• recognizing that children need adult assistance when exploring cyberspace • sharing what has been learned with a family member	information • identifying and comprehending the basic dangers of revealing personal information online to strangers • comparing strangers in the physical world with strangers online • sharing what has been learned with a family member.	passwords, user IDs, and personal information, and minimizing/evaluating pop up ads); understanding that computers can be damaged by viruses from email or the internet • demonstrating an understanding of how to use email and the internet safely • sharing what has been learned with a family member.
2-4	**Grades 2-4 student proficiency may include:** • joining online communities or games with supervision • creating and responding to emails and accessing email attachments • showing awareness of age-appropriate online communities • creating and posting content online (text, photos and audio) • searching for and downloading music safely and legally • using the mobile phone to communicate with family members and emergency services where appropriate • understanding the work of others is their property that cannot	**Grades 2-4 student proficiency may include:** • communicating appropriately using ICT with others, such as IM, email, texting, multiplayer games • demonstrating an understanding of cyberspace as a community of real people • comparing the social conventions between those of the real world and cyberspace • demonstrating an understanding of the similarities and differences between real world and online communication with ICT • defining cyber-bullying and understanding how it may affect themselves and others • communicating to an adult	**Grades 2-4 student proficiency may include:** • understanding the concept of cyber-citizenship • following social conventions and guidelines when using ICT • understanding that anyone met exclusively online is a stranger • understanding the concept that there are inappropriate places online • using safe searching techniques to locate and download content • understanding the risks of revealing personal information using ICT • demonstrating the ability to	**Grades 2-4 student proficiency may include:** • describing the basic threats to computers from the internet such as viruses, worms and trojans • understanding the concept of viruses and malware being spread from email attachments and internet sites • recognizing the security risks associated with communication devices such as email, the internet and mobile phones • sharing information with parents to check on personal computer security.

Grade Levels	Digital Media Literacy	Positive Online Behavior	Peer and Personal Safety	e-Security
	be taken without giving credit • showing awareness of age-appropriate online communities.	when a negative message is received.	make informed choices about revealing information while online • demonstrating an understanding of how to avoid or exit inappropriate places (turn off monitor, tell adult, close window, use back button) • sharing what has been learned with a family member.	
Grades 5-6	**Grades 5-6 student proficiency may include:** • developing the capacity and competence to connect to, operate and access various digital technologies and services • understanding the nature of different types of digital services and the content they provide • initiating accounts for online communication or games with supervision • participating in age-appropriate online communities • creating and responding to online content (text, photos and audio) in different forums • searching for and downloading	**Grades 5-6 student proficiency may include:** • developing the capacity and competence to connect to, operate and access various digital technologies and services • understanding the nature of different types of digital services and the content they provide • initiating accounts for online communication or games with supervision • participating in age-appropriate online communities • creating and responding to online content (text, photos and audio) in different forums • searching for and	**Grades 5-6 student proficiency may include:** • understanding the risks of revealing personal information using ICT • understanding that those met online are strangers and may be a threat to personal safety • understanding appropriate online contact and who to maintain contact with • recognizing and reporting inappropriate behavior by an online stranger to an adult or family member • recognizing and reporting when they have encountered	**Grades 5-6 student proficiency may include:** • identifying viruses, worms, trojans and spyware as programs that can damage a computer • implementing basic techniques to prevent viruses, worms, trojans and spyware infection • demonstrating safe use practices when using the internet, email and communication devices to avoid spam/scams.

Grade Levels	Digital Media Literacy	Positive Online Behavior	Peer and Personal Safety	e-Security
	music safely and legally • using a mobile phone/hand-held device to communicate with family members, friends and emergency services where appropriate • understanding the need for basic safety rules when texting or instant messaging • demonstrating a simple way to cite a source found on the internet • recognizing when 'it is too good to be true'; for example, online competitions, spam, phishing, polls.	downloading music safely and legally • using a mobile phone/hand-held device to communicate with family members, friends and emergency services where appropriate • understanding the need for basic safety rules when texting or instant messaging • demonstrating a simple way to cite a source found on the internet • recognizing when 'it is too good to be true'; for example, online competitions, spam, phishing, polls.	inappropriate content online • demonstrating an understanding of how to avoid or exit inappropriate sites (including reporting to authorities such as the teacher, school or the ACMA) • discussing online activities with a family member • acting responsibly by caring for their own and others' identity and personal information.	
Grades 7-9	**Grades 7-9 student proficiency may include:** • participating positively in age-appropriate online communities • creating an appropriate online personal profile and keeping it secure • creating, posting and responding to online content (text,	**Grades 7-9 student proficiency may include:** • communicating appropriately using ICT with others, including using the mobile phone appropriately, including SMS, MMS, internet and online games • demonstrating an understanding of cyber-bullying	**Grades 7-9 student proficiency may include:** • learning about basic safety tips to protect themselves online • demonstrating an understanding of how to avoid online predators • understanding appropriate online contact and who to	**Grades 7-9 student proficiency may include:** • describing the basic threats to computers from the internet such as viruses, worms and trojans • understanding how to protect their computer from viruses and malware

Grade Levels	Digital Media Literacy	Positive Online Behavior	Peer and Personal Safety	e-Security
	photos and audio) • analyzing online content to ensure that it is valid/trusted • synthesizing online content, including citation of owners and creators of content • understanding the term 'file-sharing' and its uses • understanding intellectual property issues and acting accordingly • recognizing dubious offers; for example, online competitions, spam, phishing or polls.	as a negative behavior • defining cyber-bullying behavior: ○ anonymity and pseudonyms (masquerading as others) ○ flaming (heated, emotive arguments) ○ harassment (denigration of others) ○ outing (public release of others' personal information) ○ exclusion (making another an 'outcast') • identifying behavior and resources available if being cyber-bullied, limiting bullying and finding help if victimized • understanding the importance of bystander awareness, knowing where to turn for help when students see a classmate engaging in self-destructive behavior or threatening suicide • understanding the concept of	maintain contact with • researching data and mobile phone plans • subscribing safely to social networking sites, peer-to-peer services and multiplayer online games • considering user agreements when subscribing to online sites • discussing family policy on appropriate website access with family members • understanding the importance of maintaining private information and the concept of a digital footprint. • recognizing that some information sites, blogs, and social networking profiles may convey mis-information and dangerous information that encourages self-destructive behaviors (e.g., eating disorders, suicide, drug abuse).	• demonstrating basic prevention and maintenance steps to protect computer firewall and update the operating system and virus protection • demonstrating safe use practices when using the internet, email and communication devices to avoid spam/scams. • describing and practicing strategies for securing wireless connections (e.g., connect only to legitimate wi-fi hot spots or turn off wi-fi, turn off file share mode, encryption of sensitive data/information, use and update of anti-virus software, use of a firewall, and update of operating system).. • advocating for secure practices and behaviors among peers.

Grade Levels	Digital Media Literacy	Positive Online Behavior	Peer and Personal Safety	e-Security
		ethical online behavior • maintaining a balanced approach to ICT use • exercising informed choices in online and digital media and communications environments • demonstrating understanding about laws on online behavior and plagiarism.		
Grades 10-12	**Grades 10-12 student proficiency may include:** • contributing positively to online communities • identifying legal and social consequences of negative behaviors, such as cyber-bullying • publishing online content using multiple tools, for example blogs, wikis, photo sharing tools • analyzing online content to ensure that it is valid/trusted • synthesizing online content from multiple sources including citation of owners and creators of content	**Grades 10-12 student proficiency may include:** • observing social conventions when using ICT to communicate with others, including the internet, phone and handheld technologies • describing the outcomes of cyber-bullying and the protective behaviors to counteract it • comprehending the potential for online harassment during e-communication • understanding the role of mobile phones in online harassment • identifying the local resources available if being cyber-bullied or	**Grades 10-12 student proficiency may include:** • identifying the various types of online relationships that can occur • comprehending the implications of willing participation in risky online behavior • understanding the positives and negatives in using social networking sites • researching data and mobile phone plans and selecting best value ones • subscribing safely to social networking sites, peer-to-peer	**Grades 10-12 student proficiency may include:** • demonstrating a commitment to stay current on security issues, software, and effective security practices. • demonstrating a commitment to stay current on security issues and effective security practices. • modeling secure practices within a variety of digital communities.understanding the security risks associated with downloading items online • demonstrating safe use practices when downloading or

Grade Levels	Digital Media Literacy	Positive Online Behavior	Peer and Personal Safety	e-Security
	• using taxonomies effectively to organize and classify multiple information sources • recognizing dubious offers; for example, online competitions, spam, phishing or polls.	stalked • identifying legal and social consequences of negative behaviors, such as cyber-bullying or harassment • understanding consequences for those who participate in online harassment • demonstrating behavior and resources to cope with cyber-bullying • understanding consequences of unethical behavior • maintaining a balanced approach to ICT use.	services and online games • understanding user agreements when subscribing to online sites • subscribing to service sites requiring payment; for example, online games • discussing family policy on appropriate web site access with family members • creating appropriate online personal profiles and keeping them secure.	sharing information online to avoid spam/scams • advocating for secure practices and behaviors among peers and community. • understanding how personal information may be compromised via spyware • sharing safe use practices with friends and family • having an adequate level of knowledge and skills to be able to protect themselves and their families from unwanted, inappropriate or unsafe content • Describe and practice strategies for managing everyday hardware and software problems.

GLOSSARY

Acceptable use policy
Documents created by schools or other organizations to outline what is acceptable behavior when using computer facilities and other technologies such as mobile phones.

Acronyms
Internet acronyms are shorthand ways of communicating that are used specifically on the internet or cell phone texting. They are popular because they save people time in preparing messages. It is quicker, for example, to type in one acronym that is easily understood, than a series of words. Example: G2G (got to go), LOL (laughing out loud)

Attachment
A file of information that is sent with an email. It may contain text, photos, graphics, sound or video.

Avatar
An icon or picture that represents a participant in online chat, in forums and in games.

Bandwidth
Bandwidth refers to how much data can be sent through an internet connection. It is usually measured in bits-per-second (bps). The higher the bandwidth, the faster users can surf the web or download files.

Blog (Web + Log)
The term 'blog' is derived from the combination of 'web' and 'log'. Blogs are virtual journals created by individuals and stored on the internet. Blogs generally consist of text and images and tend to appear in a chronological format. Find an excellent video about blogs here: http://www.youtube.com/watch?v=NN2I1pWXjXI

Bookmark/favorites
A placeholder that helps you locate a website later. Web browsers let you 'bookmark' any site and save these bookmarks in a file to recall at any time. Some browsers use the term 'favorites' to describe this function.

Bluetooth
A wireless networking technology that enables data to easily transfer from one device to another in close range without the use of cords and wires, such as cell phone to laptop computer, or headset to cell phone.

Bounce-back
Bounce-back refers to the auto-return of an email message because of an error in its address or delivery.

Broadband
Sometimes referred to as high-speed internet, broadband is an 'always on' fast connection to the internet. Broadband can be fiber optic, ADSL, DSL or wireless.

Browser
A web browser is a software program that allows you to browse the internet by simple 'point and click' navigation. Common browsers are Firefox, Internet Explorer (IE), Chrome. The world wide web is made up of millions of sites that each have their own unique address (URL). The web browser interprets coded language and presents it in an easy-to-view form that allows us to read text, view images, watch movies and listen to sound on a website.

Cache
A cache is a stash of digital files. Web browsers hold copies of recently visited web files in the computer's memory. This disk memory space is called the cache. It offers the advantage of much quicker loading when files are stored on disk than when they must be transferred from the web every time. Search engines like Google also store caches of websites that preserve the information even if it's deleted.

Case sensitive
Case sensitive means that capitalization matters. Some passwords are 'case sensitive' meaning 'ABC' is considered different data from 'abc'. Passwords that are case sensitive need to be typed in exactly the same way each time.

CD-ROM
Compact Disk-Read-Only Memory. A compact disk can store large amounts of information and is accessed by being inserted into a computer's CD-ROM drive. CD-ROM is like DVD but holds much less information.

Chat
Online chat is the informal 'conversational' communication between users of the internet while they are online. This can be direct one-on-one chat using tools such as instant messaging (IM), chat rooms or SMS. It can also be text-based group chat through mediums such as Internet Relay Chat, online forums and Wikis.

Chat room
A chat room is a place on the internet where people with similar interests can meet and communicate together by typing messages on their computer. People can often enter an unmoderated chat room without any verification of who they are. Problems for students can arise with chat room participants pretending to be someone they are not.

Cookies
Computer cookies are small files placed on your computer when you visit a website. The website saves a complementary file with a matching identification (ID) tag so it can recognise you by matching the cookie with the website's copy. Cookies keep track of information entered at a site. For example, if you submit a registration form or wish to complete online transactions, the site will match that information to your computer the next time you visit. While cookies can be turned off, they are generally not dangerous to users, and some websites may not operate correctly without the use of cookies.

Cyberbullying
Online harassment, or cyberbullying, involves the use of information and communication technologies, such as email, mobile phone text messages, instant messaging (IM) and defamatory personal websites, to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm or humiliate others.

Cyberspace
A term used generally to describe where internet transactions take place and the different experiences available through the global online world of computer networks. For example, one might describe sending an email to their friend as sending it 'through cyberspace'.

Database
A collection of data records. On web databases, records may consist of web pages, graphics, audio files, newspaper files, books, movies or anything from very general to very specific areas of interest. Database records are usually indexed and come with a search interface to find records of interest.

Demo software
Demo software is a trial version of a software program that allows people to use it for free while they decide whether or not to buy it. Generally, demo software can be downloaded directly from the manufacturer's website. The most common ways to offer demo software is to allow customers to download a complete version that will expire in a set period of time. See also, Shareware.

Download
To download a file means to transfer it from one computer to your computer. This can refer to a music file, document or photo, transferred from a website or the internet to a computer.

DVD-ROM
A Digital Versatile Disk (DVD-ROM) is a media or data storage disk that closely resembles a CD or compact disk, but is formatted to hold far more data such as movies or a television series.

E-crime
Criminal activity where a computer or other electronic communications device, such as a mobile phone, is used to commit an offence, be the target of an offence or act as a storage device in an offence. Also referred to as "internet crime."

E-commerce
Business that is conducted online.

E-security
E-security covers a range of activities to keep electronic information secure. This can include protecting a personal computer as well as protecting personal and sensitive information such as passwords and bank account details.

Email (electronic mail)
Email is a mail message that is sent from one computer to another. Email messages can be sent to anyone with an email address, anywhere in the world.

Emoticons (Emotions + Icons)
Emoticons are combinations of punctuation marks used to convey facial expressions as a shorthand method of communicating emotions through text. Emoticons can be used in any communication over the internet but are particularly popular in chat rooms and instant messaging. Examples:
:-) [smiley face], :([sad face], ;) [wink] Viewed sideways!

External (portable) hard disk-drive
An advanced version of the floppy disk, this is a disk drive that is plugged into an external port on a computer such as a USB. A portable hard disk allows the user to back up or store important information separate from the main internal hard drive, which could become compromised by online or offline activities. It is also capable of storing much more information than an internal hard drive.

FAQ (frequently asked questions)
FAQs are documents that list and answer the most common questions on a particular subject.

Filter
A filter manages access to online content. A filter can restrict times when the internet can be accessed and also restrict what is viewed and downloaded, based on certain key words or types of content. Some filters can also be instructed to specifically block information from being displayed. Types of filters range from those on home computers to filters used by a school on its server.

Firewall
Firewalls are computer systems that limit and stop access to computers by unauthorized people or other computers. A personal firewall can be installed to protect a computer from intruders. Firewalls also help to stop the spread of viruses and spam and can be a valuable tool in protecting children online.

Flame
Mean, obscene, or harassing messages sent through online chat, social networking sites, in chat rooms, IM, and cell phone texting.

Flaming
Sending mean or obscene messages that include bad language or obscene content. Flaming, also known as 'flame wars', generally occurs in unmoderated chat rooms. The majority of chat rooms remain 'open', where messages are posted automatically with no human intervention.

Freeware

Software that is offered for free to download.

Gaming
Playing an animated game. Some games are available on CD-ROM or on video game consoles such as a Wii or Xbox, while others are available directly online and can be played by more than one user, simultaneously. The software is usually based on traditional game categories, such as adventure, role-playing or strategy

GPS
A Global Positioning Satellite is a device that uses a system of worldwide navigation via satellites to pin point an exact location.

Grooming
Online grooming occurs when an adult takes deliberate actions to befriend and establish an emotional connection with a child in order to lower the child's inhibitions with the intent of later having sexual contact. It may include situations where adults pose as children in chat rooms or social networking sites and 'befriend' children in order to make arrangements to meet with them in person.

Hacker
A 'hacker' is someone who breaks into computer systems and performs other destructive or illegal acts with computers and networks.

Homepage
The first web page (or landing page) of a website.
Hyperlink
A hyperlink is any text or graphics on a website that, when clicked on, will take you to another web page or another part of the same web page. Hyperlinks ususally show up underlined and in blue.

ICANN (Internet Corporation for Assigned Names and Numbers)
To reach another person on the Internet you have to type an address into your computer—a name or a number. That address has to be unique so computers know where to find each other. ICANN coordinates these unique identifiers across the world so that we can enjoy one global Internet.

Identity theft
Identity theft is when personal information is stolen and used for fraudulent purposes.

Information and communications technology
Information and communications technology (ICT) is the term used to describe all the hardware (computers, mobile phones, cables, networks) and software (websites, computer programs) that allows data to be digitally processed, stored and communicated.

Infrared
Used to transmit data, infrared is a wireless technology that uses the range of invisible radiation wavelengths longer than the color red in the visible spectrum. Infrared can be used to transmit files or documents, but the most common infrared technology is used in remote controls for television sets and other electronic devices.

Instant messaging (IM)
Messages sent in rapid succession from one computer to another by means of small 'pop-up' windows. They are a form of 'instant email' and are very popular with students and adults alike. They are usually a one-to-one communication medium, although some programs allow many people to chat at the same time, like a private chat room.

Internet
The internet is a system of linked computer networks. It facilitates data transfer and communication services across the world. These include email and the World Wide Web.
Internet service provider (ISP)
A company that provides access to the internet for home and business users. For a monthly fee, the service provider enables people to log onto the internet and browse the world wide web and send/receive email.

Leet (Elite + Speak)
Specialized jargon specific to an online community.

Log-in (noun or verb)

A log-in (noun) is the account name used to gain access to a computer system, or (verb) the act of connecting to a computer system by entering a username and password.

Lurk
To lurk is to listen in to a mailing list, chat room or newsgroup without participating. Newcomers are encouraged to lurk for a while as they get the feel of a site and how it operates.

Keylogging
Keylogging is the use of either a hardware device installed on a keyboard or spyware software to record every keystroke made on that computer. A keylogger records everything the user types, including emails, log-in names, passwords, credit card numbers and/or bank account websites in order to steal the information.

Massively Multiplayer Online Role-Playing Game (MMORPG)
Games that can be played over the internet, with multiple players located anywhere in the world. The games allow the user to play a role within the game, usually with an avatar to represent the player. MMORPGs include The Sims Online and World of Warcraft.

Mobile Internet-enabled Devices
Mobile internet-enabled devices include phones and PDAs that are able to access the internet, upload and download information, take photographs and sometimes record sound.

Modem
Short for modulator/demodulator. A modem is used between a computer and a phone or coaxial cable line to convert the computer's digital signal to an analog signal for the line and vice versa. A modem is essential for a computer to access the internet.

MP3 Players
MP3 players are used to play MP3 audio files. 'MP3' is a type of compression technology that minimizes the size of audio files. MP3 players can keep large amounts of music in the one convenient and portable location.

Micro-blogging
Blogging or journaling in very small increments, usually less than 150 characters per post. Micro-blogging sites (exampls: Twitter.com) are social networking websites where people can send out regular updates about their daily activities. Users of micro-blogging sites can both share their updates and follow others. See an excellent video on micro-blogging here: http://www.youtube.com/watch?v=ddO9idmax0o

Netiquette (Net + Etiquette)
Netiquette describes 'the rules' of common courtesy for how people should act online, especially in forums and chat rooms. Netiquette can also be applied to email and chat.

Newbie
A newbie is a newcomer to the internet. These people may reveal their inexperience through lack of knowledge of internet conventions such as internet vocabulary, netiquette and general know-how. A common newbie *faux pas* is THE USE OF ALL CAPS which denotes screaming to experienced users.

Online Forums (Newsgroups)
Online forums are a place where people can contribute to a discussion by leaving a message of interest. Online forums exist on thousands of topics and are useful for building online communities and bringing people together with similar interests. Moderated forums are the safest to use.

Online/Offline
Being 'online' means being connected to the internet. People communicate online by sending and receiving information via email, instant messaging or chat rooma. Offline refers to activity when not connected to the internet.

Open Source Software
Open source software is software for which the programming code is available to the users so that they may read it, make changes to it, and build new versions of the software incorporating their changes.

Password
A password is used to gain access to areas on the internet where you may wish to protect or restrict access to personal information.

Passwords should be carefully protected. Use long and random passwords for any application that provides access to your personal identity information, including logging onto your computer or your social networking profile. Avoid dictionary words as a password. Ideally, the password should be eight or more characters in length. Passwords should be changed regularly.

Personal Digital Assistant (PDA)
A PDA is a hand-held portable computer. These technologies may contain digital calendars, address books, a memo pad and other accessories for both business and personal use.

Peer-to-peer (P2P) Networking
P2P is an application that runs on a personal computer; it shares files, such as music and video files, with other users across the internet. P2P networks work by connecting individual computers together to share files instead of having to go through a central server. P2P file-sharing opens your computer to severe security threats to your computer and any networks connected to it. P2P is also

Pharming
Pharming is the act of redirecting a website's traffic to an illegitimate site. Hackers establish these fake sites to gain access to personal information, such as bank account details and passwords. Users may be able to avoid pharming by ensuring they use secure web connections to access websites that require personal information, such as your bank's website.

Phishing
Phishing is sending email that is specifically designed to trick people into revealing personal information. Many phishing emails claim to be from a bank, online retailer, or credit card company. These email direct recipients to a website that looks like the real website of a retailer or financial institution, which is designed to encourage the visitor to reveal financial details such as credit card numbers, account names and passwords, or other personal information. See an excellent video on phishing
here: http://www.youtube.com/watch?v=sqRZGhiHGxg.

Photo Sharing
Photo sharing allows a user to transfer their digital images to a site on the internet so that they are able to share them with others privately or publicly. Common photo sharing sites are: Flikr and PhotoBucket. See an excellent video on photo sharing
here: http://www.youtube.com/watch?v=vPU4awtuTsk

Plug-in
A plug-in is a small piece of software that adds features to a larger piece of software, for example an audio plug-in that allows your web browser to play music.

Plug-and-play
Add-in hardware that has been designed for users to buy it, bring it home, plug it in and start playing. This is hardware that has been designed to identify itself on most computers, so that installation is less complicated for the user.

Podcast and Vodcast
A podcast is a digital audio file made available on the internet for downloading to a personal audio player, such as an MP3 player. Podcast files can range from music files to segments of radio broadcasts. Vodcasting is the video version of a podcast. See an excellent video on podcasting
here: http://www.youtube.com/watch?v=y-MSL42NV3c

Pop-ups
Pop-ups are small windows that appear in the foreground of an internet browser. Pop-ups can be integrated into some websites for practical purposes, however they are often used to display advertising or pornography on the screen. Most web browsers have a setting to block pop-ups.

Privacy Policy
A privacy policy outlines the terms by which a company or website handles personal information from its visitors to the site. Privacy policies can often be found as a text link in the footer section of a web page.

Profile

Information about a user. A profile may contain details such as the user's name, address, interests and pictures. Profiles are commonly used on social networking websites or when customising the information received from a website. Children should be careful not to provide information on their profiles that can easily identify them or their location.

RSS Feed (RSS)
Really simple syndication (RSS) feeds, also called 'newsfeeds', allow web users to keep up to date with news headlines or blogs. With an RSS reader, you can scan hundreds of news headlines from one location. After signing up to a website's RSS feed, users receive notices in their reader anytime that the website is updated. See a video explanation of RSS
here: http://www.youtube.com/watch?v=0klgLsSxGsU.

Safe Zones
Safe zones are an alternative to filtering or labelling. Labelling allows web developers to categorise online content on the basis of language, violence, sexual content etc. Safe zones are services providing access to a range of sites that are suitable for children.

Search Engine
A search engine is a website that searches the information available on the internet. Some search engines work by automatically searching the contents of the web and creating a database of the results. Other search engines contain only material manually approved for inclusion in a database and some combine the two approaches. See an excellent video on Web search strategies: http://www.youtube.com/watch?v=CWHPf00Jkgg

Shareware
Shareware is software that is offered for free to download in the hope that the user will decide to keep it and pay a fee for it after trying it out.

Social Networking Websites
A social networking website is an online place where a user can create a profile and build a personal network of online 'friends'. In the past five years, sites such as MySpace and Facebook have engaged tens of millions of internet users. See a social networking video here: http://www.youtube.com/watch?v=6a_KF7TYKVc
See a Social Media video
here: http://www.youtube.com/watch?v=MpIOCIX1jPE

Spam
Unsolicited commercial, unwanted email messages usually advertising a product or service.

Spyware
Spyware is a computer program that can be installed on personal computers, usually without the permission of the owner that collects information and sends it back to another source. This can often be an internet marketing, pornographic or gambling website. Spyware can also be used maliciously to steal your log-in and passwords for secure websites, such as online banking.

Streaming Audio and Video
To 'stream' an audio or video file is to listen to or watch audio or video in real-time as the content is downloaded to your computer from a remote website.

Surf
To browse or explore the internet with no specific purpose.

Tagging
A tag is a word, or a group of words, assigned to a piece of information, such as a picture, article or video clip, that allows the user to describe the content of the item and to search and cross-reference information online. For example, users can 'tag' an article they read on a newspaper website with 'news', 'funny' or 'car'. It is important to note that tagging does not use a centralised vocabulary for classifying information—tags are determined by users.

Thread
A series of messages with the same subject. It consists of an original message and all the replies that follow. People can both respond to the original message or to each other in a 'threaded discussion'.

Troll

An outrageous message posted on a forum, chat site or wiki designed to bait people to answer. Trolling is a form of harassment that can take over a discussion. Well-meaning defenders can create chaos by responding to trolls. The best response is to ignore it.

Update/patch
A patch is an update that fixes problems ("patching the holes") within software programs. Programmers design patches to fix small bugs, glitches or operating system compatibility issues. In most cases patches are free and the majority are simply downloaded from the internet.

Upload
To upload a file is to transfer a file from your computer system to another computer or system via the internet.

URL (Uniform Resource Locator)
URL is the address of a website or file. They usually begin with www (World Wide Web), followed by the name of the company or product.

User
A user of the internet or information and communication technologies and products. For example, people can be described as website users or computer users.

Username
An alias or 'handle' used specifically for online interactinos. When you sign up for a service such as Hotmail or a chat room, you are required to create a unique identifier—a username—that helps to protect your identity. For example, 'maz123'.

Virtual Reality
A computer simulation of a real three-dimensional world, often supplemented by sound effects. Examples include 3D flight simulators or first-person games where you explore 3D 'worlds'.

Virtual Worlds
Virtual worlds are simulated worlds created on the internet that people can visit from their computer. 'Residents' can create a new identity known as an avatar and interact with other avatars in real-time in a relatively lifelike social setting. Popular virtual worlds include Second Life (adults) and WoogiWorld and Club Penguin (children).

Virus and Anti-virus
A virus is a computer program designed to cause undesirable effects on computer systems. Viruses are often disguised as something else so that they can be transferred undetected from one computer to another. They can be hidden in emails, on CDs or in files that are shared across the internet. Computer viruses can cause harm to computer systems and need to be avoided. Anti-virus software can be installed on computers to scan for and remove computer viruses.

VOIP (Voice Over Internet Protocol)VOIP is a technology that allows voice communication to be transmitted via the internet in the same way one might use a telephone to make a phone call. Popular use of VOIP technology is through the software Skype or Google video chat which allows users to make video and phone calls via the internet to anywhere in the world.

Web Page
A web page is a file or content accessible on the internet by requesting a single URL.

Webcam
A camera attached to a computer that transmits real-time still and video images to others via the internet.

Web 2.0 (Two Point Oh)
Web 2.0 is the general term given to describe the second generation of internet communication where users create and upload their own content, rather than simply view (or download) static websites. New web products, such as blogs, wikis,video sharing, RSS feeds, and social networking have created this new environment where people join communities to collaborate and share information online.

Wi-Fi (wireless) Internet Access

Wireless networking technology uses radio waves to provide wireless high-speed internet and network connections.
Wi-Fi works with no physical wired connection between sender and receiver by using radio frequency technology. In order to connect to an access point and join a wireless network, computers and devices must be equipped with wireless network adapters.

World Wide Web
The World Wide Web or 'web' as it is more commonly called, is a collection of pages on the internet that can be read accessed with any web enable devise such as mobile phone, PDA and computers. Users need an internet connection, a computer, a web browser, in order to access and interact with the online information that forms part of the web.

Wikis
Wikis are an online group of documents/web pages that many different users can add to and edit freely online. The most famous wiki is Wikipedia. However, users of wikis cannot always assume information is correct—there can be errors and bias in the information presented. See an excellent video presentation on wikis here: http://www.youtube.com/watch?v=-dnL00TdmLY,

Common internet acronyms
ASL? = Age, sex, location?
BFF = Best friends forever
BFN = Bye for now
BRB = Be right back
CUL8R = See you later
G2G or GTG = Got to go
JAM = Just a minute
LOL = Laughing out loud
POS = Parents over shoulder
ROFL OR ROTFL = Rolling on the floor laughing